Manchester City Council
Report for Information

Report to: Human Resources Sub Group – 4 February 2016

Subject: Employment Policies

Report of: Head of HROD Service Delivery

Summary

This report is intended to update Members on the HR workplan and includes proposed revised employment policies Internet and E-mail and the Domestic Violence and Abuse Policy. These policies have been updated to include recent developments in legislation, social and organisational changes.

Details are included on forthcoming policy changes/developments in respect of Adoption Leave and Pay, Recruitment and Selection and the Management of Attendance Policies.

Recommendations

The HR Sub Group is asked to note and provide comments on the revised policies.

Wards Affected:
All

Anti-poverty	Equal Opportunities	Environment	Employment
No	Yes	No	Yes

Contact Officers:

Name: Pat Fetherstone, Head of Service Delivery
Tel: 0161 234 1847
E-mail: p.fetherstone@manchester.gov.uk

Name: Mallicka Mandal, Employee Relations Manager
Tel: 0161 219 6365
E-mail: m.mandal@manchester.gov.uk

Background documents (available for public inspection):

The following documents disclose important facts on which the report is based and have been relied upon in preparing the report. Copies of the background documents are available up to 4 years after the date of the meeting. If you would like a copy please contact one of the contact officers above.

N/A

1.0 Introduction

1.1 This note sets out revisions to a number of the Council's employment policies. These are the Internet and Email Policy and Domestic Violence and Abuse Policy. These policies have been revised following legislative and organisational factors which make existing arrangements out of date.

1.2 The HR Sub-Group is requested to provide comment and feedback prior to the revised policies being submitted for consideration by Personnel Committee on 2 March 2016.

1.3 Subject to formal approval, these policies will come into effect 1 April 2016 and publicised to the workforce and managers through broadcasts with links to the policy and guidance on the Intranet. Where staff do not have access to the electronic systems, managers will be requested to cascade the information through team meetings.

1.4 Once formally adopted by Personnel Committee each of these policies will replace existing arrangements as set out below:

a) The Internet and E-mail Policy, once formally approved, will replace the separate Internet/Intranet Policy and Guidance and the E-mail Policy and Guidance, both implemented in 2007.

b) The Domestic Violence and Abuse Policy, once formally approved, will replace the existing Employee Domestic Abuse Policy approved by Personnel Committee at its meeting on 28 March 2007.

2 INTERNET AND E-MAIL POLICY (Appendix 1)

2.1 The Information Commissioners Office (ICO) visited Manchester City Council to undertake an audit of information governance (IG) practices, policies and procedures in December 2014. The subsequent report highlighted a need for regular review of IG related policies to ensure they are clear and robust. Reviewing the internet and email policies was seen as an opportunity to address the issues raised in the ICO report and to modernise the approach to the hitherto separate policies on Internet/Intranet and E-mail.

2.2 Whilst developing the current draft, research was conducted into approaches of other organisations on internet and email use; input and suggestions were invited from trade unions, service managers, legal, audit and ICT.

2.3 An Equality Impact Relevance Assessment was conducted which found that there was a positive impact as a result of the review of the policy, in that there are now clear and robust messages around the sanctions for employees who use the email and internet tools for or connected with discriminatory purposes.

2.4 Once approved formally, this single policy will replace the hitherto separate policies on internet and email which were implemented in 2007.

2.5 The key features in the revised policy are:

- Merging of Internet and Email policies into one easy to read document
- Introduction of document control cover per the ICO recommendations

- Links to relevant Information Governance policy and pages included per ICO recommendations
- Strong message throughout the policy on information security
- Terms for personal use of both email and internet are specifically clarified

2.6 The review of the internet and email policies in line with ICO recommendations reduces the risk to the Council of abuse or incorrect use of these tools. Employees will benefit from clarification about information governance and the additional guidance which will accompany the policy on the intranet.

2.7 A plain English summary for employees also accompanies the policy. This is has been developed by the Communications Team to communicate the key policy messages.

3. DOMESTIC VIOLENCE AND ABUSE POLICY (Appendix 2)

3.1 Context

One in four violent crimes involve people in domestic relationships and it is estimated that one in four women and one in six men will experience domestic violence and abuse at some time in their lives. There were over 19,500 Domestic Violence and Abuse crimes recorded by Greater Manchester Police from residents in Greater Manchester in 2014/15.

The Council is committed to ensuring that any employee who experiences domestic violence and abuse can raise the issue at work, without fear of stigmatism or victimisation, and will receive appropriate support and assistance.

The policy has been developed in consultation with the Domestic Abuse Reduction Co-ordinator and other relevant stakeholders. Feedback from the trade unions, Independent Domestic Violence Advice Service, Public Health and the Equalities Team has been incorporated into the revised policy.

It is envisaged that this Policy will have a positive impact on the health and well-being of the workforce and support the campaign to reduce domestic abuse across Greater Manchester as a key employer in the region.

3.2 Main Changes

3.2.1 Whilst the principles established in the previous Domestic Abuse Policy are still sound, there are aspects that require updating in line with guidance from the Equality and Human Rights Commission.

3.2.2 The revised Domestic Violence and Abuse Policy includes a policy statement along with an updated Home Office definition of domestic violence and abuse, guidance for managers on identifying, responding to issues and for the provision of support for employees experiencing domestic abuse. It also covers the need for confidentiality, monitoring and signposts to support available. The Council's approach to dealing with employees who are found to be perpetrators of domestic violence is also set out.

3.2.3 Whilst confidentiality is of the upmost importance, there are situations when a manager may be obliged to disclose the information to the Council's

Independent Domestic Violence Advice Service, for example if the employee is considered to be at risk of significant harm or death. The Independent Domestic Violence Advice Service will assess the information provided and will decide whether a referral to the Multi Agency Risk Assessment Conferences (MARAC) should be made. MARAC holds monthly multi agency meeting involving local social care representatives. This element has been incorporated into the policy.

3.2.4 A full Equality Impact Assessment has been conducted and as the policy has a high relevance to employees with protected characteristics under equality legislation. As a result the policy now includes a revised monitoring form which will support future capture of equality monitoring information against the policy and enable the organisation and relevant stakeholders to develop strategies to address these.

4.0 Employment Policies in Development - Progress Update

4.1 Adoption Leave and Pay Policy

The Work and Families Act 2006 introduced statutory adoption leave and pay provisions for employees. It was introduced by the Government as part of its policy to give parents more choice in balancing their work and family lives. These provisions were changed by the recent Children and Families Act 2014, which came into force on 5 April 2015.

The key legislative changes comprise:

- Statutory adoption pay brought into line with statutory maternity pay by setting it at 90% of normal earnings for the first six weeks of the adoption pay period, followed by 33 weeks' at £139.58 (current statutory rate set by the government).
- Prospective adoptive parents entitled to take time off "for the purpose of having contact with the child or for any other purpose connected with the adoption".
- The 26 weeks qualifying period for adoption leave was removed, so that it mirrors the eligibility requirements for maternity leave.
- Eligible employees who take adoption can are also now able to 'opt' into the new Shared Parental Leave scheme.
- Surrogate parents and foster parents are now eligible for adoption leave.

A revised Adoption Leave and Pay Policy has been drafted to take account of legislative changes and also to look at the best approach to encourage adoption and fostering. Further guidance to enable employees to understand the arrangements will also be included within the draft policy supported by Frequently Asked Questions, Process Flows, Glossary of Terms etc.

The current draft is being consulted on and comments are currently awaited from the Head of Fostering and Adoption on the proposed approach. An Equality Impact Assessment is also underway on the revised arrangements.

It is envisage that the draft policy would be ready for the forthcoming HR Subgroup meeting to be held in March 2016.

4.2 Recruitment and Selection Policy

Recent financial settlements have resulted in a significant reduction in external recruitment and an increased focus on internal matching and movement to promote skills development and continuous learning. Nevertheless, external recruitment is still a vital aspect of the Council's overall resourcing arrangements and is used to recruit for critical or specialised and senior roles, with the policy guiding these processes and decision-making. This has been the driver behind the recent refresh of the arrangements with the production of a more modern, up to date and flexible framework.

There has been significant new legislation since 2003 which impacts on the previous arrangements including the Equality Act 2010, Safeguarding Children and Vulnerable Adults, Data Protection, Right to Work etc. The impact of these changes has been incorporated into the draft policy and associated guidance.

In addition to legislative changes there has been considerable structural and functional transformation in the organisation along with changes to operating procedures since 2003. These include the move away from prescriptive job descriptions and person specifications to role profiles, the emphasis on career pathways and job families, the focus on safeguarding and safe recruitment to roles working with children and vulnerable adults. The refreshed policy takes account of all these developments.

In developing this policy, research has taken place to consider recruitment and selection policies of other organisations including local authorities. This has found a significant move away from prescriptive process-driven approaches to a more adaptable one that allows recruitment and selection arrangements to be applied flexibly to fit operational requirements, whilst maintaining a core set of principles, rooted in the Council's values to guide these decisions and ensure that recruitment is professional, fair and ethical .

The draft policy will include a suite of documents that provide more detailed guidance for managers including "How to" guides for managers on assessments methods, interviewing and scoring, references etc.

The draft policy has been widely consulted and comments received are being incorporated. However, further consultation needs to be undertaken on the safeguarding aspects of the policy with the Head of Safeguarding. An Equality Impact Assessment is also being undertaken to ensure compliance with the Equality Act 2010.

It is anticipated that the final revised Recruitment and Selection Policy will be ready by early March 2016.

4.3 Management of Attendance

Management of Attendance is a key priority for the Council. The existing arrangements need updating in line with legislative and organisational changes. These changes include the Equality Act 2010, changes in Retirement on health grounds provisions due to amendments to Pension Scheme Regulations, changes in the way we provide Occupational Health Services etc. Additionally, the approach to managing attendance has shifted

within the organisation with increased emphasis on prevention, reasonable adjustment and line manager and service accountability.

The revised policy addresses absence from a health and well-being perspective providing guidance for managers and employees on identifying and addressing health issues early. Clear frameworks and timeframes have been implemented to address disability related absence and long term sickness, which outlines the comprehensive support available for each. These frameworks adhere to the current legislation in these areas and seek to encourage attendance via support and adjustments where required.

An early draft of the policy was circulated at the Health and Wellbeing Steering Group, which comprises senior service managers, trade unions, public health representatives, health and safety and HR officers. Comments are awaited and expected to be received and incorporated by early February 2016. The intention is that final draft will be tested with a number of managers to assess their view of its practical application and ease of understanding. Accompanying guidance is also being drafted to further support managers and employees.

5. Next Steps

5.1 The HR Sub-group is also requested to provide comments on the Internet and E-mail and the Domestic Violence and Abuse Policy described in sections 2 and 3.

5.2 It is proposed that the final draft Management of Attendance policy will be presented to the HR Sub-Group for comments at the forthcoming meeting on 2 March 2016.

5.3 A view is sought from the HR Sub-group on potential dates for presenting the remaining Adoption Leave and Pay Policy and the Recruitment and Selection Policy.

[DRAFT]
Internet and Email Policy

Employee Relations Team
HROD
March 2016

MANCHESTER CITY COUNCIL

www.manchester.gov.uk

Document Control

Title	Manchester City Council – Internet and Email Policy
Document Type	Policy
Author	Employee Relations Team
Owner	HROD
Subject	Internet and Email
Date created	August 2015
Approval date	(tbc)
Review date	Two years from the date of approval (or earlier where there is a change in the applicable law)

TABLE OF CONTENTS

1 Introduction

2 Purpose and Scope

3 Aims

4 Information Security

- Passwords Filtering
- Software
- Access

5 Monitoring

- Individual
- Shared
- Archiving

6 Intranet

7 Internet

- Non Permitted Uses
- Personal Use

8 Email

- Non Permitted Uses
- Personal use

9 Public Access

10 Role and Responsibilities

- All Users
- Managers

11 Sanctions for misuse

12 Declarations

Appendix 1 - Categories of Blocked Websites
Appendix 2 - Using Email securely - Guidance
Appendix 3 - Relevant Legislation
Appendix 4 - Summary Guide for Employees

1. Introduction

1.1 E-mail and internet are important business communication tools, but it is important to remember that these are still subject to the same business, legislative and accountability requirements as other written communications, including laws on data protection, freedom of information, defamation, harassment, copyright, obscenity, fraud and wrongful discrimination.

1.2 The following Internet and Email Policy is one of the Council's most vital policies. It supports the Council's Information Security (IS) Policy (and its Code of Practice) which are based on the British and International Standards for Information Security, and complies with all relevant legislation and best practice guidance provided by the Information Commissioners Office (ICO) and other government agencies.

1.3 The Council is committed to upholding the laws relating to information and systems. Relevant legislation can be found in the Information Security Policy and Information Security Guidance on the Council's ICT intranet pages.

2. Purpose and Scope

2.1 The purpose of this policy is to set out the standards for the management and acceptable use of internal and external email and internet/intranet systems in order to meet the Council's legal and business requirements.

2.2 This policy applies to all directly employed Council employees, agents and contractors with access to Council ICT facilities.

2.3 Where the Council acts as a data processor/agent on behalf of other individuals/organisations using the Council's email communication system, the conditions of use will be set out in the terms of the contract.

2.4 All users are expected to comply with the policy when using the Council's email and internet/intranet facilities, whether accessed locally or remotely.

2.5 This policy should be read in conjunction with the Council's Social Media Policy, Employee Code of Conduct and the Disciplinary Policy pg 19-21 all of which can be found on the HROD intranet pages.

2.6 Failure to adhere to this internet and email policy may result disciplinary action see part 10.

3. Aims

3.1 The aims of this policy are to ensure that:

- corporate standards and legal guidelines for managing and using these tools through the Council's ICT facilities are established and consistently enforced
- the Council is protected against liability for the actions of its employees
- users of electronic systems are educated about the legal risks involved in electronic communications
- damage to ICT systems is prevented
- unnecessary time spent on non work related activities is avoided or reduced
- users are aware of the privacy and security expectations when they draft, send or receive communications
- business records are managed and retained on the basis of their content, not format
- internet and email users are protected by clarifying:
    - the requirements for information security
    - the purpose and extent to which the Council monitors the use of these tools
    - prohibited and unacceptable uses
    - the requirement to agree to the policy on a periodic basis
    - the consequences for breaching the policy

4. Information Security

4.1 The Council has a duty to its service users, customers, contractors, suppliers and employees to ensure their confidential information is protected. The user's obligations are made clear under the policy. This will minimise the risk of breaching this duty, whilst also preventing misuse of the email and internet/intranet facilities.

4.2 Before using the email or internet/intranet systems, users must be familiar with this policy, understand the Information Security Code of Practice (found on the ICT intranet pages) and must follow any specific instructions given by their line manager or the ICT service regarding any aspect of the Council's computer systems. For further information on ICT security and the Golden Rules around protecting information please see the following link http://intranet.mcc.local/protectinginformation/Pages/Default.aspx

4.3 When using email and internet accounts in the work place, users must always be aware of and uphold their responsibility to protect information, remembering

to lock screens when away from desks, use appropriate passwords, secure unused devices and under no circumstances allow anyone other than themselves to access their work email or internet/intranet accounts.

4.4 Where employees access their Council email account or internet/intranet system remotely or from home, they must have robust and adequate security measures in place to ensure information is protected and cannot be accessed by unauthorised persons. Devices must not be accessible to anyone other than those authorised to use them and equipment must be made secure to prevent loss or theft.

4.5 Employees must not send confidential data, business information or any information relating to their work to their own or anyone else's personal email address.

4.6 Data sent or shared via the Council's email or intranet/intranet systems, whether on site or remotely, should be for business purposes only.

4.7 The methods chosen to communicate confidential information must be consistent with the Council's obligations to safeguard sensitive personal information to avoid accidental breaches of personal data.

4.8 Confidential email communications, particularly of sensitive personal information, should utilise encryption software or secure email accounts.

4.9 The Council accepts no liability for the actions of staff who decide to use the Council's email or internet systems to send personal data about their private lives Staff are directly responsible for meeting any relevant obligations under the Data Protection Act 1998 in this regard. For further information on the Councils expectations surrounding the use of Social Media please see the following link http://intranet.mcc.local/hrod/Pages/SocialMediaPolicy.aspx .

4.10 Staff need to be aware that misuse of work's email or internet facilities in a way which breaches any of the requirements of this policy or the Information Security Code of Practice could lead to formal action under civil/criminal law and/or their contract of employment.

Passwords

4.11 A unique user identity and password will be assigned where access to email and internet/intranet facilities is provided to employees in order to facilitate council business. For more information on passwords please read Part 5 of the IT Access Control Policy (Appendix 5). Passwords are simple to operate and if used carefully can prevent unauthorised access to data. Following a few simple rules can make it difficult for unauthorised people to gain access to the Council ICT systems:

- Never reveal your password
- Never ask anyone else to reveal their password to you
- Under no circumstances share your password
- Never write your passwords down
- Do not use your own, your partner's, your child's or your pet's name, your telephone number or anything else that is easily recognisable as a password

- Always remember to lock your screen/device when not in use to prevent unauthorised access

Filtering Software

4.12 To protect the email network, email messages are scanned by software to identify spam and viruses. The Council deploys automatic message monitoring, filtering and rejection systems as appropriate, and this software denies transmission of messages that may breach the terms of this policy.

4.13 Filtering software is also used to prevent access to internet sites which are not work related and which the Council considers to be inappropriate. Details of the categories of sites which are blocked are attached at Appendix 1 and include streaming media.

Access

4.14 All emails sent or received over the Council's network for business purposes belongs to the Council and forms an integral part of the Council's business records. Therefore, access to email accounts is provided via the Council's corporate network only.

4.15 Access to the internet is also provided via the Council's corporate network only.

4.16 PCs, laptops, terminals or any ICT equipment must be connected to the internet through this corporate network, unless the formal written approval of the ICT Head of Service Operations has been obtained.

4.17 Employees working from home or remotely must access the internet or email through the corporate network using one of the means of remote access approved and supported by the ICT Service.

4.18 Attempts to access the internet in a way which circumvents controls is monitored through software installed on all PCs, laptops and other ICT equipment.

5. Monitoring

5.1 As permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Network Security Team in the ICT Service maintains, on behalf of the Council, appropriate monitoring arrangements in relation to all Internet, email and related services and facilities that it provides. For further details please refer to the Information Security Code of Practice.

5.2 Software is also installed to identify and report on all web sites accessed by each internet user. Reports on staff accessing, or attempting to access, non-work related internet sites will be communicated to line managers upon request.

5.3 To protect the email network, email messages are scanned by software to identify and deny transmission of messages considered to conflict with the terms of this policy.

5.4 Filtering and monitoring measures may highlight potential internet misuse. Cases of internet misuse will be investigated in accordance with the Council's disciplinary procedures.

Individual

5.5 The Network and Security Team will provide reports to Heads of Service on the top 50 websites accessed by internet users where requested. In addition the Network and Security Team will provide internet activity reports on the top 50 internet users in departments, again where requested.

5.6 Managers are entitled to access their team's email accounts:

- to ensure business requirements and standards are met when employees are in attendance, or absent from work unexpectedly or for prolonged periods
- to investigate complaints
- where unlawful activity and/or breach of contract is suspected, including email misuse and/or abuse of privileges granted for personal e-mail users

Shared

5.7 Where service provision requires it and for business continuity reasons, a manager may request that an employee is provided with access to another employee's email account. Where this occurs, managers must ensure that the employees involved are aware of the access granted to their accounts.

5.8 Under no circumstances is an internet account to be shared between employees without the relevant authorisation. User names and passwords are unique to each employee. Those without access can request an account via the "request a service" link on the Council's ICT intranet page.

5.9 Managers must ensure that access to an employee's email account by other employees is limited only to those who require it for business purposes.

5.10 Access to emails labelled 'PERSONAL' may take place where a manager concludes this is necessary and proportionate, where there are reasonable grounds for suspecting unlawful activity and/or breach of contract, including email misuse and/or abuse of privileges granted for personal email use.

5.11 Requests for access to the content of emails labelled 'PERSONAL' or internet usage may arise in relation to a disciplinary matter or an ongoing investigation. Such requests may come from a manager, the Network Security Team or other relevant council staff including officers in HROD or Internal Audit for the purpose of an ongoing investigation or a disciplinary matter. All such requests must be made by email in the first instance to HROD to consider. The request, the reasons behind it and the extent and duration of access, should be set out clearly. The requesting officer will be required to comply with the IC Security Access Procedure in order to get access to this information.

5.12 Should there be a requirement to investigate the breach of this policy, HROD will liaise with the Head of Internal Audit and Risk Management or the City Solicitor who are authorised to approve specific reports from ICT on individual email and internet use

Archiving

5.13 The E-mail Archiving system ensures all sent and received email, including internal email messages are automatically captured and retained in the email archive. E-mails are copied into the archive at the time of transmission/receipt and will remain in the archive, regardless of whether the user deletes the email from view in their personal mailbox.

5.14 This means that all emails held in this system are potentially "disclosable" on request under subject access related legislation. This underlines the importance of ensuring that appropriate language and professional care is used in all email correspondence.

5.15 Further information on record keeping requirements and the retention and disposal of business records will be available from the departmental/service records manager or from the Democratic Services Legal Team.

6. Intranet

6.1 Manchester City Council has an internal electronic communication and information system referred to as the "intranet" which can be made available to anybody attached to the corporate network. This system provides information on directorates, policies and procedures, an A to Z directory of staff and various other information and updates.

6.2 The content of the intranet relates directly to Council business and access is not limited or filtered.

6.3 Employees are expected to act responsibly whilst using the intranet and not to spend time browsing unnecessarily.

7. Internet

7.1 The Internet is a worldwide network linking millions of computers and which contains information on almost any topic. Internet users are capable of viewing and transmitting information and electronic mail worldwide.

7.2 The content of the internet does not relate directly to Council business and as such access is limited and filtered.

Non-permitted uses

7.3 Employees will not be permitted to use the Council's internet facilities to:

- set up or maintain personal web sites

- participate in chat rooms, forums or social media for reasons other than business purposes for more information, see the Social Media Policy at http://intranet.mcc.local/hrod/Pages/SocialMediaPolicy.aspx
- access auction sites, for example eBay
- gain unauthorised access to systems
- bring the Council into disrepute
- breach any Policy of the Council, its objectives or values
- operate or manage any private business, commercial/profit making activities and/or activity for personal financial gain
- place commercial, promotional or advertising material
- knowingly expose the system to viruses and/or junk-mail/spam
- infringe the copyright of another person, including intellectual property rights
- waste staff effort or networked resources
- deny service to other users
- access, download, transmit or store text, images or other material which could be considered:
  - sexist, racist, homophobic, xenophobic, pornographic or of a sexual nature, pedophilic, discriminatory or offensive
  - in conflict with their role within Manchester City Council
  - unlawfully discriminatory, libelous or defamatory
  - contain material that includes claims of a deceptive nature
- involve unauthorised disclosure to a third party of personal information about a service user or council employee
- create internet based email and instant messaging accounts for personal use

NB This is not intended as an exhaustive list and does not presume that all other uses are automatically acceptable, see page 19-21 of the Disciplinary Policy on the following link http://intranet.mcc.local/hrod/Documents/Disciplinary%20Policy.pdf

Personal Use

6.4 The Council is prepared to permit a limited amount of personal internet use, however, this is a privilege granted by the Council, not an entitlement and is permitted under the conditions that use of the internet for personal reasons:-

- is outside the employee's normal working hours unless specifically agreed with the line manager
- does not impact on the individual's work performance or service delivery

- does not involve the private buying or selling of any goods or services over the internet using the Council's email communication system
- does not involve the use of the Council's email address for any communication or purchases made over the internet, either from home or from a Council computer outside of working hours
- does not involve signing up to or supplying the Council's email address to non-work related mailing lists
- does not cause any expense or liability to be incurred by the Council
- does not include any attachments, or documents, which include pictures or computer software
- is in accordance with the non-permitted uses as set out at part 6.3

7. Email

7.1 Electronic mail (*E-Mail*) is simply a medium to convey information, and carries the same formality as, for example, a written memo. Therefore using appropriate professional language and refraining from personal opinion is vital when writing work related emails. In view of the potential consequences of use or misuse of email, users need to be particularly vigilant in terms of system use, system security and confidentiality.

7.2 Where confidentiality is required, using email and internet facilities may not always be the most reliable or appropriate means of communication. All laws relating to written communication apply to emails and these can be produced in court and are subject to the same statutory rights of access (i.e. data protection, environmental information regulations, freedom of information) in the same way as other kinds of written information.

7.3 Legal advice is generally confidential and attracts legal professional privilege ensuring that the solicitor/client relationship is protected under the common law, but this may not apply once advice is communicated to another party. As such, before using email, always check with your legal adviser.

7.4 Unless using encryption software, external email is vulnerable to unauthorised access and alteration as it passes over the internet. As the security of external messages cannot be guaranteed, encryption must be used for transmitting confidential data unless the explicit permission of the system manager has been given. System managers should seek the advice of the Network and Security Team within the ICT service before approving the use of un-encrypted email.

7.5 Time critical and important business external emails (e.g. tender requests, contracts etc.) should be followed up to ensure safe arrival or receipts requested. Do not assume external emails always arrive at the intended

destination. The increasing use of spam filters by all organisations makes this less certain.

7.6 Employees must ensure emails they send are addressed to the correct recipients i.e. people authorised to receive the information the employee is sharing. The email system will auto suggest names when letters are entered in the recipient box, as such, it is the employee's responsibility to make sure the intended recipients are correct before sending.

7.7 When sending group emails, employees are expected to ensure that everyone listed in the recipient box is authorised to receive the information being shared.

7.8 Employees must ensure all work-related emails sent include the originators name, job title, and contact details, as specified in Customer Care standards and set out at http://www.mcc/od/all/care/index.htm. See the guidelines on email management for advice on email etiquette. These guidelines are available on the Information Security section on the ICT area of the Councils intranet.

Non-permitted use

7.9 This policy prohibits the use of the Council's communication systems for the creation or transmission of emails that:

- bring the Council into disrepute, breach any Council Policies, objectives or values
- involve the operation or management of any private business, commercial/profit making activities and/or personal financial gain
- consist of unsolicited commercial, promotional or advertising material
- initiate or continue chain letters
- knowingly expose the system to viruses and/or junk-mail/spam
- waste staff effort or networked resources or cause disruption to the Council's communication systems by, for example, sending inappropriate emails which distract staff or sending large emails which cause the email system to crash
- infringe the copyright of another person, including intellectual property rights
- are designed, by intent or otherwise to cause annoyance, offence, inconvenience, or anxiety to anyone
- include the creation, transmission or storage of text, images or other material which could be considered
    - sexist, racist, homophobic, xenophobic, pornographic, pedophilic, discriminatory or offensive
    - conflict with their role within MCC
    - unlawfully discriminatory
    - libelous

- defamatory

- contain material that includes claims of a deceptive nature
- violate the privacy of others, or unfairly criticise or misrepresent others
- claim to come from an individual other than the user actually sending the message
- undertake, assist or encourage a criminal act
- involve unauthorised disclosure to a third party of confidential material concerning the activities of the Council
- involve unauthorised disclosure to a third party of personal information about a service user or council employee
- involve unreasonable or excessive personal use
- create internet based email and instant messaging accounts for personal use, via the Council's network

NB This is not intended as an exhaustive list and does not presume that all other e-mail uses are automatically acceptable, see page 19-21 of the Disciplinary Policy on the following link

http://intranet.mcc.local/hrod/Documents/Disciplinary%20Policy.pdf

Personal Use

7.10 Though the Council's email facilities are provided for business purposes, it is recognised that occasional use for personal purposes would be very helpful. The Council is prepared to permit a limited amount of personal use, however, this is a privilege granted by the Council, not an entitlement, and is permitted on condition that this use:

- does not impact on the individual's work performance or service delivery. Typically no more than five minutes per day sending, reading or acting on personal emails is considered to be reasonable
- does not involve the private buying or selling of any goods or services over the internet using the Council's email system
- does not involve the use of the Council's email address for any communication or purchases made over the internet, either from home or from a Council computer outside of working hours
- does not involve signing up to or supplying the Council's email address to non-work related mailing lists
- does not broadcast non-work related emails to teams, sections or groups without the permission of the head of the team, section or group
- does not take priority or interfere with the performance of the employee's duties or the work commitments of other members of staff or with use of Council's email system for business purposes
- does not cause any expense or liability to be incurred by the Council

- does not include any attachments, or documents, which include pictures or computer software
- does not conflict with the Council's objectives, values or have an adverse impact on the role of the Council in any way
- is lawful and fully complies with this policy, and is consistent with the non-permitted uses listed in part 7.9

7.11 Personal use outside these conditions is only permissible under exceptional circumstances. Staff must gain the permission of their line manager, who will inform the Network Security Team via email setting out the exact nature of the exceptions and the likely duration. Records of approval of exceptional

7.12 Data relating to personal use will be retained by the Network Security Team and scrutinised where necessary. Further guidance on good practice is available on the ICT intranet pages.

7.13 When making use of email facilities for personal correspondence, staff need to be aware that they can expect very limited privacy due to the Council's commitment to monitor communications (see part 4). They must also ensure:

- All personal email sent should be marked PERSONAL in the subject header, and all personal email sent or received must be filed in a folder marked "PERSONAL" in the employee's mailbox
- It is the employee's responsibility to ensure that anyone outside the Council, who sends a private message, identifies the message as 'PERSONAL' in the email header
- The standard staff signature i.e. the originator's name, job title, email address and contact details should be removed from all personal emails

7.14 It is important to note that emails may be viewed via a viewing panel without opening the email itself. Therefore, employees must carefully consider encrypting emails containing sensitive or private information.

7.15 Employees wishing to send sensitive information relating to their personal circumstances, for example to the Occupational Health Section or Trade Unions, may as an alternative to email send it in hard copy form by internal mail and mark it "Private and Confidential".

7.16 All email contained in an individual's mail box and the corporate archive system, not marked 'PERSONAL', are deemed to be business communications.

7.17 As with any correspondence made using the Council's electronic facilities, staff can delete personal email from their own mail box but these may be captured and stored for a defined period in a corporate email archiving system.

8. Access under FOI/DPA

8.1 Employee email and internet accounts may be accessed to retrieve information relevant to a request for information under the Freedom of Information Act 2000, the Environmental Information Regulations 2004 or the Data Protection Act 1998.

8.2 Such access will be limited to the relevant accounts required, and where possible will use specific search terms to retrieve only relevant information. Access will only be granted where the request has been approved by an authorised person.

9. Roles and Responsibilities

All Users

9.1 Employees must use the Council's ICT facilities responsibly, lawfully, with respect for recipients, and in accordance with this policy, related ICT policy, the Council's Code of Conduct for Employees and its Equal Opportunities and Employee Dispute Resolution Policies and Procedures. Any use of the email or internet facilities which is observed or reported to be in breach of these policies, or which endorses failure to uphold these policies, will be investigated in accordance with the Council's agreed disciplinary procedure.

9.2 Security of the Council's ICT systems is of paramount importance. At every log on, employees must take responsibility for their actions.

9.3 Employees must read and understand the Information Security Code of Practice and the Internet and E-mail policy especially in relation to securing devices, access to accounts, non permitted uses and preventing the breach of confidential information and data.

9.4 Employees are responsible for ensuring that their actions do not threaten the security of confidential information or compromise the integrity of the Council's ICT systems.

9.5 Employees are responsible for keeping people-related and commercially sensitive information confidential, ensuring it is only disclosed lawfully and, with appropriate authorisation. For further information on data protection see the Protecting Information page on the intranet at http://intranet.mcc.local/ProtectingInformation/Pages/Default.aspx or the Information Commissioner's web site at https://ico.org.uk/for-organisations/guide-to-data-protection

9.6 Employees are required to comply with the conditions and limitations on personal use of the email and internet/intranet systems.

9.7 All security breaches or conduct which is in conflict with this policy must be reported to a responsible manager and the Network and Security Team within the ICT Service as soon as is practicable after the incident. Please

refer to the Information Security Incident Management Procedure available on the intranet pages at the following link http://intranet.mcc.local/ProtectingInformation/Pages/Incidents.aspx

9.8 Where an employee accesses a website which they consider to be contrary to Council Policy or inappropriate they must inform the Network and Security Team in the ICT Service.

9.9 All employees have a duty to report any email received which includes unacceptable content to a responsible manager and the Network and Security Team, as appropriate.

Managers

9.10 Managers are responsible for ensuring that:

- employees have read and understand this policy
- employees are provided with clear instructions on
  - Information security
  - personal access to the internet and email
  - the need to report inappropriate websites, emails and data breaches to their line manager and where required, the Network and Security Team
- there is no detrimental effect on their service by permitting their employees to access the internet before work, at lunch breaks or after work
- there is no detrimental effect on their service by permitting their employees to utilise the email system for personal use
- employees do not use the internet for personal purposes during working hours
- their staff use the Council's email and internet system in accordance with this policy
- staff in breach of this policy are dealt with in accordance with the disciplinary policy where required

10. Sanctions

10.1 Failure to observe the requirements and fulfil the roles and responsibilities within this policy may result in the following sanctions

- disciplinary action, up to and including summary dismissal being taken under the Council's Disciplinary Procedure
- the rescinding of access to the internet and, where applicable, civil action and/or criminal charges

10.2 Any authorised user who breaches this policy, who is not employed by, or under the direct control of, Manchester City Council will be liable to any other sanctions the business relationship or law permits.

10.3 Where use of the e-mail/internet potentially breaches civil and criminal law, the City Solicitor will be informed.

11. Declaration

11.1 Upon accessing the internet for the first time, new users will be required to accept this policy indicating that they have read and agree to abide by its terms and that they understand that the Council monitors and filters systems as part of their ICT security measures.

11.2 Existing users will also be required to periodically reaffirm their acceptance of this policy via a login screen when accessing accounts.

11.3 When a user clicks the periodic screen message to agree that they have read and will abide by these policies, their agreement is recorded in an ICT database and can be retrieved for use in investigations where required.

11.4 Those who fail to sign the declaration or affirm their acceptance to abide by this policy may have their e-mail and internet accounts suspended.

Appendix 1 Categories of Blocked Websites

- Intimate Apparel & Swimwear
- Hacking
- Intolerance & Hate
- Personals & Dating
- Proxies & Translations
- Adult / Sexually Explicit
- Chat
- Criminal Activity
- Illegal Drugs
- Alcohol & Tobacco
- Gambling
- Games
- Social networking Sites (restricted access)
- Spam URLs
- Streaming Media (restricted access)
- Ringtones / Mobile Phone Downloads
- Violence
- Tasteless & Offensive
- Weapons
- Web-based E-mail
- Peer- Peer
- Phishing & Fraud

APPENDIX 2

Using Email Securely - Guidance

Revision History

Version	Date	Author	Description of change
V5.0	27 July 2015	Rebecca Taylor, Senior Solicitor (Information Governance)	Re-title, formatting, updating weblinks. Minor changes to sections 1,5 and 6.

Next Review Date: August 2018

1. Introduction

1.1 This Guidance aims to help you comply with the Council's Internet and Email Policy and to promote good data handling practice with the aim of ensuring confidentiality is not compromised when using email.

1.2 Separate guidelines under the Code of Connection apply to officers with access to the Government's Secure Intranet (GSI) sub network called GCSx. Where using GCSx or other secure email facility, any requirements issued as a condition of use will over-ride this Guidance.

1.3 Whether contacting businesses, partners or individuals it is not appropriate for MCC officers to communicate "protected information" by external email without first ensuring it is safe from (i) interception during transmission and (ii) is only accessible by the intended recipient. Generally, it is important to be aware that non business email addresses may only be used where consent has been obtained from the individual. Consent is important but does not override the Council's security obligations.

2. Definition

2.1 "Protected information" means information about people (living individuals) and/or commercially sensitive business information which if intercepted or disclosed to the wrong recipient has the potential to cause harm/distress, including damage to an individual and/or the Council's reputation.

3. Internal Email

- Always check you are sending the email to the right person – common names or similar spellings underline the importance of carefully selecting the right email address.
- Do not put the names of individuals in the email subject line.
- Only include the minimum information necessary.
- Use initials rather than full names whenever feasible.
- Only forward emails containing protected information strictly on a "need to know" basis.
- Think before using directorate/group email address lists which should only be available for use on restricted basis and subject to case by case senior management authorisation (note: some group email address lists include third parties).
- If you send an email to the wrong internal address, do not compound the error by forwarding the same email again. Send a separate email explaining the error. Ask the recipient to delete the email and to confirm to you by email when this has been done and if they managed to do this before opening/reading it.
- If you receive an internal email intended for someone else, take the following action:

- Copy and paste the sender's email address into a new email, record the time, date and subject line of the email sent to you in error. Delete the email received in error. Then notify the sender of their mistake, providing the record of the email details and the action you have taken. Ask them to correct their email contacts; inform their manager to ensure the incident is reported in accordance with the Council's incident security procedures as set out in the Information Security Incident Management Procedure.

- If the wrongly addressed email sent by you contains personal information about a person (employee, service user, customer) inform your line manager as the security incident needs to be reported.

4. External Emails

- Remember that external email travels over the public network which is not secure
- If you are sending one mail shot to multiple recipients, email addresses of individuals acting in a non work capacity may be personal data so make sure the email addresses are included in the "bcc" address line so these cannot be seen or used by other recipients
- Do not include any protected information in the email subject line or body of the email
- Ensure that protected information is contained within an encrypted attachment which has a strong password
- Make sure service users with whom you have regular email contact understand that unencrypted email transmitted over the public network is insecure and that if they choose to communicate this way, they are at least aware of the risks and try to minimise them
- Make sure that email communications to persons acting in a professional capacity (solicitor/barrister etc) are addressed to business email account and not to private email accounts, such as: "hotmail", "yahoo" etc
- If you send an email to the wrong external address, do not compound the error by forwarding the same email again. Send a separate email explaining the error. Ask the recipient to delete the email and to confirm to you by email when this has been done and if they managed to do this before opening/reading the email. Report the security breach to your manager.
- If you are made aware an email sent by you has been received by the wrong recipient which contains personal information about a person (employee, service user, customer) inform your line manager immediately as the security incident needs to be reported and investigated. Do not delete the email as the severity of the breach depends on the content of the email and the potential harm which may be caused by sending it over the public network and to the wrong person.
- If you receive a (valid non spam) email from an external source intended for someone else, take one of the following actions:

- Copy and paste the external senders email address into a new email, record the time, date and subject line of the email sent to you in error. Delete the email received in error. Then notify the external sender of their mistake, providing the record of the email details and the action you have taken
- If you know the identity of the intended Council recipient and their email address, forward the email explaining you received it in error and ask the intended recipient to ensure the sender updates their address records. Make an independent note of the date and time, subject line, name and email address of the sender, the action you have taken and then delete the email received in error from your in box and the forwarded email from your sent box.

5. How do I encrypt an email attachment?

5.1 Protection Information must be contained in a separate document. You should not include Protected Information in the email subject line or body of the external email, or in the filename of the attachment.

5.2 It is important to use the version of WinZip available through Citrix. You must follow the step-by-step instructions on the intranet which explain how to encrypt and password protect the document:http://intranet.mcc.local/cex/performance/transformation/ict/Knowledge/Email%20Attachment%20Encryption.aspx

5.3 You must use the method explained above. It is not sufficient to use the password protection options in Word or Excel as the Protected Information will not be suitably secure.

5.4 When selecting a password for the encrypted document, you should use a "strong" password that is difficult to guess. You should use a unique password each time you send encrypted information. Follow the password rules accessible from this link:http://intranet.mcc.local/cex/performance/transformation/ict/Knowledge/Password%20Rules%20for%20Active%20Directory.aspx

5.5 You should provide the recipient with the password by phone if possible. **Never** send the password in the same email as the attachment.

5.6 Always double-check the email address is correct before hitting the send button.

5.7 Emails with encrypted attachments will usually be quarantined by ICT because the email virus checker cannot scan an encrypted file. You will receive a message from ICT asking you to reply and include the password in the body of your email so the content may be viewed before it is “released” to the intended external recipient.

5.8 Always ask for confirmation the recipient has received the email safely - but when you send the email advise the intended recipient to delete the encrypted attachment first before sending an email reply confirming safe receipt.

6. Receiving Protection Information from outside the Council

6.1 If you know external parties propose to send you protected information by email, you must ask them to send this in a secure way. If you have a contractual relationship, this should form part of the security requirements specified in the contract.

6.2 If email is the only or most speedily available option, the external party must use a process similar to the Council's arrangements for sending encrypted attachments described in Section 5 above. Ensure the external party ideally phones you with the password which in any event must not be contained in the same email as the encrypted attachment.

6.3 Incoming emails containing an encrypted attachment will usually be quarantined by ICT because the email virus checker cannot scan an encrypted file. ICT will contact you for the password before releasing the incoming email to you.

6.4 Smaller external organisations might not have immediate access to "zip and encrypt" software, but this is available at low cost or free to download. The Council does not recommend particular software but for information the Council uses WinZip or 7-Zip. The recommended encryption standard is "AES 256 bit".

6.5 Individuals contacting Manchester City Council officers may choose to send Protected Information by email and to make complaints, arrange meetings or raise other enquiries with the Council in this way. Where it is known this might involve sensitive protected information (i.e. health related, financial), the risks involved should be explained and individuals should be discouraged from using email unless they use a method of encryption.

6.6 The link to the Council's Email Disclaimer is automatically appended to emails and confirms that unless encrypted, email messages passing over the internet are not secure and could be intercepted and read by someone else. Please see the following link for the full Email Disclaimer:

http://www.manchester.gov.uk/site/scripts/documents_info.php?categoryID=200031&documentID=3513

APPENDIX 3

LEGAL CONSIDERATIONS

This section gives brief information of some of the laws that might be applicable to computer use in the workplace.

Some of the laws cover the content of e-mails or sites downloaded from the Internet, other legislation covers privacy issues, monitoring of communications and surveillance at work.

HUMAN RIGHTS ACT 1998

This provides for the concept of privacy giving a 'right to respect for private life and family life, home and correspondence'. This provision is directly enforceable against public sector employers, and all courts must interpret existing legislation in relation to the Human Rights Act.

Covert Monitoring is likely to be unlawful unless undertaken for specific reasons as set out in the Regulation of Investigatory Powers Act 2000 and the Telecommunications (lawful Business Practice)(Interception of Communications) Regulations 2000. Employers need to make sure employees are aware of any monitoring or recording of correspondence.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

This Act covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunication system, and applies to public and private communication networks.

The employer is expected to make all reasonable efforts to ensure system users know that communications may be intercepted, and any such monitoring must comply with the provisions of the Data Protection Act 1998, and in particular the Data Protection principles on fair processing.

DATA PROTECTION ACT 1998 (DPA)

The Information Commissioner, who is responsible for enforcement of the Data Protection Act, has published a code of practice to help employers comply with the provisions of the Data Protection Act. The Employment Practices Code clarifies the Act in relation to processing of individual data, and the basis for monitoring and retention of email communications. The code of practice Monitoring at work: an employer's guide states that any monitoring of emails should only be undertaken where:

- the advantage to the business outweighs the intrusion into the workers' affairs
- employers carry out an impact assessment of the risk they are trying to avert
- workers are told they are being monitored

- information discovered through monitoring is only used for the purpose for which the monitoring was carried out
- the information discovered is kept secure
- employers are careful when monitoring personal communications such as emails which are clearly personal
- employers only undertake covert monitoring in the rarest circumstances where it is used for the prevention or detection of crime.

PROTECTION OF HARASSMENT ACT 1997, DEFAMATION ACT 1996, DISCRIMINATION LAW (age, sex, race, disability, sexual orientation and religion or belief)

These laws all protect individuals from suffering abuse, harassment, defamation or discrimination at the hands of others. E-mail communications and the downloading of inappropriate images from the Internet may contain language or graphics that are insulting, demeaning or unlawful. Whilst the perpetrator of the message or download may be legally liable for damage caused, the employer may also have vicarious liability for the actions of their workers.

CONTRACT LAW

It is just as possible to make a legally binding contract via e-mail as it is by letter or orally. Workers need to be aware of the danger of inadvertently making contracts on behalf of their employer, or varying the terms of any existing contract.

COPYRIGHT LAW

The Copyright, Designs and Patents Act 1988 (as amended) gives the same protection to digital and electronic publications as it does to printed books and other forms of publication. Many websites carry warnings that the information given is copyright and should not be downloaded without agreement from the copyright holder. Similarly copyright exists over software, which should not be downloaded without license.

Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

These Acts are concerned with material that might be criminal, cause harm to young persons or be otherwise unlawful. In the workplace the downloading of certain images from the Internet might subject a worker to charges of criminal behaviour.

COMPUTER MISUSE ACT 1990

This Act is mainly concerned with the problems of 'hacking' into computer systems.

Appendix 4 - Summary Guide for Employees

Introduction to the Internet & Email Policy

E-mail and internet are important business communication tools, and widely accepted as the most efficient way to make contact with, or stream information to others.

The Internet and Email Policy (I&EP) is one of the Council's most vital policies. It supports our Information Security Policy and its Code of Practice, which are based on the British and International Standards for Information Security, and comply with all relevant legislation and best practice guidance provided by the Information Commissioners Office (ICO) and other government agencies.

The I&EP includes guidance, regulations and conditions of use, and it also sets out our responsibilities. The key thing to remember is that email and internet use is subject to the same business, legislative and accountability standards as printed and verbal communications: we all need to stick to the rules and expect everything that we do by email or online to be subject to the same scrutiny as more traditional communications.

Possibly the most important detail is the section about online safety and keeping sensitive information safe. We should all be aware of the Internet Security Code of Practice, and understand that there are vulnerabilities in even the most robust systems, so our day to day practice needs to be mindful of any potential lapse.

Within the I&EP there are sections relating to:

Aims

Setting out why we need this policy, who it applies to and what it hopes to achieve.

Information Security

Detailed section focussed on our duty to protect the information we keep, prevent the unauthorised sharing of information, and prohibited use of the internet and email.

Passwords

Outline of the protocol for passwords, and how to keep them safe.

Filtering software

To uphold our responsibility for protecting information, we filter all incoming and outgoing information.

Access

Guidance on giving access to your email.

Monitoring

Statement about monitoring of internal/external communications, including situations in which monitoring is authorised, why and how the detail is stored for future use e.g.: investigations or complaints.

Individual/shared accounts

Setting out why colleagues may need access to your account and how / when to do this properly. Also detail about why it's important not to share without the proper authority.

Archiving

The storing of information and what it can be used for.

Internet/intranet

Outline of appropriate use of each.

Personal use

Guidelines for personal use, limits and standards of behaviour. Also details our responsibility to report unauthorised personal use that breaches any of the guidelines e.g.: excessive, discriminatory, offensive or racist.

Email protocol

Looks at content and language, and disclosure of information.

Encryption

When this can and should be used and the potential consequences of failing to encrypt information that's emailed.

Sensitive/protected information: incoming and outgoing, internal and external.

This section of the policy is essential reading for all employees: we all need to understand data protection legislation to the extent that it applies to each of us when sharing information. Includes detail about reporting inappropriate sharing of sensitive information, intentional or accidental.

Please take the time to read through the Internet & E-mail Policy: much of its content is common sense and you may consider yourself to be fully aware of the rules, regulations and potential pitfalls.

But the risk of making mistakes, leaving the entire organisation open to criminal activity is very real, so protect us all by protecting yourself.

MANCHESTER
CITY COUNCIL

Domestic Violence & Abuse Policy (DRAFT)

Employee Relations Team
HROD
March 2016

www.manchester.gov.uk

Document Control

Title	Domestic Violence and Abuse Policy
Document Type	Policy
Author	Employee Relations Team
Owner	HROD
Subject	Policy and Guidance on Dealing with Domestic Violence and Abuse
Date Created	November 2015
Approval	tbc
Review due	Two years from the date of approval (or earlier where there is a change in the applicable law).

Table of Contents

1 Policy Statement

2 Definition

3 Aims

4 Legal Obligations

5 Impact of Domestic Violence and Abuse on the Workplace

6 Provision of Support

- Confidentiality
- Safety in the Workplace

7 Employees who are Perpetrators of Domestic Violence and Abuse

8 Recording and Monitoring

Appendix 1 Support, Help and Advice for employees experiencing or perpetrating Domestic Violence and Abuse

Appendix 2 Checklist for Managers: Responsibilities following a disclosure of domestic violence and abuse

Appendix 3 Monitoring Form

1. Policy Statement

One in four violent crimes involve people in domestic relationships and it is estimated that one in four women and one in six men will experience domestic violence and abuse at some time in their lives. There were over 19,500 Domestic Violence and Abuse crimes recorded by Greater Manchester Police from residents in Greater Manchester in 2014/15. Statistics show that women victims are more likely to be sexually abused, to experience repeated and sustained abuse and more likely to be murdered, whereas male victims are less likely to access existing services and often fear ridicule should they disclose abuse at the hands of a woman.

Lesbian, gay, bisexual and transgender people experience domestic violence and abuse at about the same rates as heterosexual women, however, the problem is often underreported. Those involved in same gender abuse are often afraid of revealing their sexual orientation or the nature of their relationship due to fear of being 'outed' by the abuser or the fear that support structures such as service providers or the legal system are inherently homophobic.

Domestic violence and abuse occurs across society, regardless of age, gender, race, sexuality, wealth and geography and it has extreme consequences for victims across a whole range of outcomes, including physical and mental health, alcohol use, homelessness and in extreme cases, murder.

Domestic violence and abuse involves misuse of power and exercise of control by one adult over another adult; usually within the context of an intimate relationship or within a family. It can take many forms such as physical assault, bullying, sexual abuse, rape and threats. It can also include or take the form of psychological and emotional abuse and include destructive criticism, pressure tactics, disrespect, control of finances and contact with friends and family members, breaking trust, isolation and harassment. It also includes forced marriage where marriage is performed without the consent of both individuals, and honour crimes which are committed to protect or defend the honour of the family or community.

It is recognised that domestic violence and abuse is an issue that can impact on the workplace. It can affect the morale, health, well-being and self-confidence of an employee, which in turn can impact on their performance at work. Assisting and supporting individuals to resolve difficulties in their personal life will have a positive effect on their performance at work.

According to the Corporate Alliance Against Domestic Violence, a nationally recognised charity, domestic violence and abuse currently costs UK business over £1.9 billion a year due to lost economic output through decreased productivity, absenteeism, errors and increased employee turnover. Colleagues may also be affected by having to cover a survivor's workload or feeling unable to help when they know there is a problem.

Manchester has one of the highest rates by population of domestic violence and abuse and the Council is committed to ensuring that any employee who experiences domestic violence and abuse can raise the issue at work, without fear of stigmatism or victimisation, and will receive appropriate support and assistance.

2. Definition

From March 2013, the government has defined domestic violence and abuse as any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality. This can encompass, but is not limited to, the following types of abuse:

- psychological

- physical
- sexual
- financial
- emotional

Controlling behaviour is: a range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating their everyday behaviour.

Coercive behaviour is: an act or a pattern of acts of assault, threats, humiliation and intimidation or other abuse that is used to harm, punish, or frighten their victim.

This definition, includes so called 'honour' based violence, female genital mutilation and forced marriage, and is clear that victims are not confined to one gender or ethnic group.

3. Aims

The aim of this policy is:

- To ensure that all employees, not only those experiencing domestic violence and abuse, are aware of the Council's policy and its implications, including its implications for employees who are perpetrating domestic violence and abuse.
- To assist and support employees who ask for help in addressing domestic violence and abuse issues.
- To provide guidance to managers on how to support and assist employees asking for help in addressing domestic violence and abuse issues and how to deal with employees who are perpetrators of domestic violence and abuse.
- To ensure that employees seeking assistance are confident their situation will be handled sympathetically and confidentially.
- Reduce absences from work resulting from domestic violence and abuse and have a positive impact on employees' mental and physical health and well-being.

4. Legal Obligations

The Council recognises that all its employees have the right to feel safe within their working environment. This policy supports the health and well-being of Council employees by:

- Providing a safe working environment for all employees (Health and Safety at Work Act 1974)
- Enables the Council to act in accordance with the European Convention on Human Rights (Human Rights Act 1998)
- Provides for the well-being of its residents (Local Government Act 2000)
- Enables compliance with the Crime and Disorder Act 1998
- Enables compliance with the Domestic Violence, Crime and Victims Act 2004.

5. Impact of Domestic Violence and Abuse on the Workplace

An individual who is experiencing domestic violence and abuse may choose to seek advice/support from a number of sources, including their immediate supervisor or another member of direct line management. If approached, managers need to be prepared to listen, to be sensitive and non-judgemental in order that the most appropriate help can be offered. Managers need to be aware of the signs, ask questions and show concern for employees and should bring the existence of this policy to the attention of their staff.

In the event that the individual is not comfortable with approaching their manager as an initial contact, the employee may seek the support of a colleague or Trade Union representative who may make the initial contact on their behalf.

People experiencing domestic violence and abuse may feel stigmatised and disempowered. There may be individual contextual factors that affect how willing or able they are to seek help. They may not want to admit or share their experience because they feel some responsibility for the situation, they feel shame, or they feel they should be able to deal with the situation on their own. There can also be fears that they will not be believed, they may have fear of the consequences, or their experiences will be trivialised and that they will cause trouble for the perpetrator.

Domestic violence and abuse can have a significant impact on mental health and is a common factor in the development of depression, anxiety and other mental health disorders which in turn can impact on attendance at work and ability to seek help, therefore identifying that an employee is experiencing difficulties at an early stage can help ensure that appropriate support is provided and help the employee to deal with their situation more effectively. This can reduce repeated work absences and can ultimately reduce the extent of the domestic violence and abuse experienced.

Managers should create an environment where employees feel safe and able to talk about issues that are affecting them. They need to consider the possibility of domestic violence and abuse if an employee is visibly injured, depressed, distressed or unusually lacking in self-confidence and self-esteem.

Other indicators could be:-

- Increased absenteeism or lateness;
- Excessive clothing;
- Repeated injuries or unexplained bruising;
- Uncharacteristically depressed, anxious, distracted or lacking in concentration;
- Loss of confidence or self esteem;
- Changes in the quality of work for no apparent reason;
- Receiving repeated upsetting telephone calls/faxes/e-mails;
- Obsession with time;
- Avoiding lunch breaks or socialising outside work;
- Reluctance to leave work at the end of the working day;
- Isolating themselves at work;
- Repeatedly requiring time off for appointments;
- Substance misuse issues;
- In the case of forced marriage or honour based domestic violence and abuse – excessive parental or family restrictions, control of movement, control of income, limited choices

It may also be the case that the employee discloses information about domestic violence and abuse as part of other discussions e.g. during an appraisal interview, informal discussion about performance, sickness absence etc. It may be appropriate for Managers to bring this policy to the attention of the employee during a return to work interview or other private discussions.

6. Provision of Support

Having the issue raised with them, managers should be able to advise the employee of available sources of support, including access to counseling, referral to appropriate agencies, involvement of the police etc. Managers should encourage victims to speak to specialist agencies who can risk assess and provide advice on safety planning or other support. Victims who disclose should be allowed to contact services from their workplace.

Details of the support and services provided in respect of advice and referral to both men and women suffering domestic violence and abuse are attached at Appendix 1.

It is vital that employees have the chance to think through all the available options and decide for themselves how they wish to handle matters. Therefore managers should pay considerable regard to the employee's views before deciding how to proceed.

Support and assistance should be tailored to the individual employee's needs and requests so far as possible. This recognises that each individual will have different needs at any one time and that these needs can vary over time for the individual concerned. However, all support should be given bearing in mind the needs of the service.

In addition to the immediate assistance and counselling referred to above, requests for time off from employees who are experiencing domestic violence and abuse may be made in relation to:

- Appointments with support agencies, welfare agencies and legal advisors;
- Arrangements for re-housing;
- Making arrangements for children and any other dependants where necessary, including schools;
- Attending relevant court hearings.

These requests should be treated sympathetically and be subject to the same criteria that normally apply to requests for special leave. Consideration should also be given to temporary variations to hours or patterns of work as appropriate.

Confidentiality

The Council respects an employees right to confidentiality. Confidentiality can be crucial in maintaining an employees safety from further abuse. Anyone who becomes aware that an employee may be experiencing domestic violence and abuse should take this into account when responding to the disclosure.

The Council recognises that employees experiencing domestic violence and abuse normally have the right to confidentiality. However in circumstances where there is a belief that the individual is at risk of significant harm or death, or which involve the safeguarding of children or adults at risk, complete confidentiality cannot be guaranteed. If the Council is informed that an employee or a vulnerable member of their immediate family is at risk of significant harm, the employee will be informed at the first opportunity that a disclosure has been made and encouraged to access the support available.

If an individual is thought to be at risk of significant harm or death, the manager should consider a referral to the Multi Agency Risk Assessment Conferences (MARAC) using the Manchester Domestic Violence and Abuse Referral and Assessment Form and sending this to the Council's Independent Domestic Violence Advice Service. The Independent Domestic Violence Advice Service will assess the information provided in the referral form and will decide whether a referral to MARAC should be made. MARAC holds monthly multi agency meeting involving local social care representatives. Further advice on this can be sought from the Councils' Independent Domestic Violence Advice Service.

The Manchester Domestic Violence and Abuse Referral and Assessment Form is available from the Council's internet site at:

www.manchester.gov.uk/info/200036/domestic_violence/550/get_help_and_advice_about_domestic_abuse/3

Confidentiality will therefore be upheld in line with the following terms:

- All advice, information and support will remain confidential. No information or documentation should be disclosed without the express consent of the employee unless there is an immediate safeguarding or child protection concern.
- The manager must gain consent from the individual to share any information; except in cases where there are potential risks to the protection of children that must be reported.
- All meetings with employees should take place in private and any information recorded should be kept in secure storage.
- Employees experiencing domestic violence and abuse may be accompanied at meetings, if so desired, by a colleague, trade union representative or friend.
- Where issues regarding child protection or the protection of vulnerable adults from abuse arise, the child protection and the adult protection services may need to become involved.
- Where a manager becomes aware that another employee may be responsible for an act of domestic violence and abuse they will need to report these concerns to the relevant Service Manager. See Section 7 for further details.
- Managers are reminded that information with regard to home address or change in home address or telephone number of any employee should not be divulged without the express consent of the employee.
- Employees have the right to a private life. If an employee does not wish to inform the Council that they have experienced domestic violence and abuse, they have the right to privacy. However, it is only possible for the Council to facilitate a range of support with domestic violence and abuse issues, if the person discloses abuse to their manager or to another manager or gives permission for someone else to do so.

Safety in the Workplace

The Council's Violence to Staff Policy will apply to most situations of abuse in the workplace. Once a manager is made aware of domestic violence and abuse the manager should discuss with the employee whether there is any risk to the employee whilst at work. If the employee believes this to be the case, the manager should seek advice from Health and Safety in carrying out a risk assessment and taking action to minimise risks in the workplace. For example, additional security measures at the entrance to the building, interception of telephone calls etc, moving the employees work station away from the view of a window, or changes to work patterns or location to address any risks identified when travelling to and from work.

Incidents of harassment or unwanted contacts at work should be reported using the Council's Violent Incident Report Form.

7. Employees who are Perpetrators of Domestic Violence and Abuse

All employees should be aware that domestic violence and abuse is a serious matter that can lead to criminal convictions. An employee who is a perpetrator of domestic violence and abuse will be in direct contravention of Council policy and may be subject to disciplinary action (up to and including summary dismissal).

Any employee who is responsible for giving advice or support to sufferers of domestic violence and abuse or is responsible for policy work in this area needs to be particularly aware of the potential consequences if they are found to be perpetrators of such behaviour. Given the nature of their work they will be considered to have had full understanding of the impact and consequences on the victim, and therefore the Council expects high levels of probity from employees working within these services. Managers within these relevant areas must ensure that expectations surrounding the expected levels of conduct outside of work are clearly defined and communicated to staff.

Conduct constituted as domestic abuse or violence (whether or not it leads to a criminal conviction) may lead to disciplinary action against an employee because of its employment implications and because it undermines the confidence the Council (as employer) has in the employee and may bring the Council into disrepute.

Where a manager becomes aware of such conduct, there should be as thorough an investigation undertaken as possible, a view taken and a consideration of whether the conduct is sufficiently serious to warrant disciplinary action being taken (up to and including summary dismissal).

Factors to take into account when considering disciplinary action will include the following:-

- The nature of the conduct;
- Job role – the impact of the employee's actions on their duties and responsibilities; and any Safeguarding issues that arise
- The impact on the victim or his/her dependents

An employee who is a perpetrator of domestic violence and abuse may approach their line manager about their own behaviour and the manager should offer advice about the services available to perpetrators of domestic violence and abuse (see Appendix 1).

8. Recording and Monitoring

Where any instances of domestic violence and abuse are reported to them, managers should complete a monitoring form (see Appendix 2) and return it to the HROD Employee Relations Team under confidential cover. The form does not capture any personal details. It will be used to monitor the instances of domestic violence and abuse and the assistance/support provided to the employee. This information can then be used to inform future reviews of this policy and the support available to employees.

Support, Help and Advice for Employees

National Services

For refuge accommodation or outreach support (and general advice and support around Domestic Violence and Abuse) contact:

National Domestic Violence Helpline
(24 hours/7 days a week)
0808 2000 247

If you are gay, lesbian, bisexual or transgender and experiencing Domestic Violence and Abuse, contact:

Broken Rainbow Helpline
(Monday to Friday 9 a.m.–5 p.m.)
0300 9995428

If you are being (or have been) forced or coerced into a marriage and need help, support and advice, then you can contact:

The Forced Marriage Unit at the
Foreign and Commonwealth Office
020 7008 0151 - Monday to Friday 9 a.m.–5 p.m. For outside of these hours, call 020 7008 1500 and ask for the Foreign Office Response Centre.

Men's Advice line – advice and support for men experiencing domestic violence and abuse.
0808 801 0327.
www.mensadviceline.org.uk

Samaritans 08457 909090
Open 24 hours a day. They offer confidential emotional support. This can be by telephone, email, letter and face to face for people in distress.

City-wide Services

Independent Domestic Violence Advice Service

The service involves the professional provision of advice, information and housing related support to survivors of Domestic Violence and Abuse living in the community, about the range, effectiveness and suitability of options to improve their safety and that of their children. This advice is based on a thorough understanding and assessment of risk and it's management, where possible as part of a multi-agency risk management strategy.

The service aims to work with people to maximise their potential to live as safely and successfully as possible in their environment. We will do this by empowering individuals through direct support and the engagement of services appropriate to the needs of each individual.

Tel: 0161 234 5393
Fax: 0161 274 7129

http://intranet.mcc.local/adults/teams/homeless/Pages/Independent%20Domestic%20Violence%20Advice.aspx

If you have been raped or sexually assaulted, contact:
St. Mary's Sexual Assault Centre (24 hours/7 days a week)
0161 276 6515

For men affected by sexual abuse, for advice and support contact:
Survivors UK on 0845 122 1201 Monday and Tuesday 7 pm – 9.30 pm or
Thursday 12 pm – 2.30 pm.

For refuge accommodation or outreach support in the North West (and general advice and support around domestic violence), contact:
Manchester Women's Domestic Violence Helpline
(Monday to Friday, 10 a.m.- 4 p.m.)
0161 636 7525

For emergency accommodation in Manchester, contact:
The Homelessness Advice and Assessment Service is 0161 234 4692.
The Out of Hours number for all services is 0161 234 5001.

The 'Sanctuary scheme'

The 'Sanctuary scheme' is for people who could become homeless because of domestic violence. It helps you stay living in your home, and to feel safer by fitting free security measures. It doesn't matter what type of housing you live in – council, housing association, renting from a private landlord, or a home you own. It's a partnership between the City Council, the police, fire service and Safe Partnership - a national charity that helps people vulnerable to violence and crime

To find out more contact the 'Independent Domestic Violence Advice Service' on 0161 234 5393, email: **domestic.violence@manchester.gov.uk**

The Manchester NHS City-wide Domestic Violence Project End the Fear website offers online information, advice and support for anyone experiencing, or supporting someone experiencing Domestic Violence and Abuse: www.endthefear.co.uk

Victim Support offers information and support to victims of crime or witnesses of crime:
0845 456 8800 or online at info@victimsupport-citymcr.co.uk

Local Refuges and Outreach Services

For safe refuge and support there are six refuges in the Manchester area:-

1. Central Manchester Women's Aid
   0161 820 8419
2. South Manchester Women's Aid
   0161 820 8418
3. Saheli Asian Women's Refuge.
   0161 636 7551. Service includes 'Hosla' Asian Women's Outreach Project
4. Sojurners House:
   0161 860 8421
5. Wythenshawe Women's Aid

0161 860 8420

6. North Manchester Women's Aid
0161 860 8417

Even if the Manchester refuges cannot provide you with accommodation, then the Manchester Women's Domestic Violence Helpline or the National Helpline will be able to support you to find suitable refuge space in other areas.

There are confidential community-based outreach support services for women who have experienced or are experiencing Domestic Violence and Abuse. Help includes telephone support, advocacy, face to face meetings at community settings, including venues like Sure Start Children's Centres, support with letter writing/form filling, signposting to other agencies and aftercare support for women who have been re-housed in the area.

The Manchester Women's Aid provides a city wide refuge and outreach service, the contact details are 0161 860 7999 and email address is www.manchesterwomensaid.org/

If you are experiencing domestic violence, information about how to access support, help and advice is available in some South Asian languages through the Community Helpline Language Service at the Women's Domestic Abuse Helpline**, 0161 636 7525** / email: **helpline@independentchoices.org.uk**

Manchester Women's Aid in partnership with Barnados, Manchester MIND and Eclypse provide the Big Manchester programme which delivers support for families with children aged 5-11yrs, experiencing Domestic Violence and Abuse substance misuse and mental health issues.

Tel: 0161 795 0795 or email: bigmanchester@barnados.org.uk
Manchester Women's Aid provide a citywide service for 15 – 25yr old women through the Safe Choice Worker. www.manchesterwomensaid.org

Police

If you have been the victim or witness to Domestic Violence and Abuse, or have concerns regarding a victim of Domestic Violence and Abuse, there are several ways you can report this. If you find yourself in a situation where you are in immediate danger, phone 999. Alternatively you can call your local Specialist Domestic Violence and Abuse Investigators http://www.gmp.police.uk/.

Bury Public Protection Investigation Unit: 0161 856 8064
Monday – Friday 7am to 8pm
Saturday and Sunday 8am to 4pm

North Manchester Public Protection Investigation Unit: 0161 856 3704
Monday to Friday – 7am to 8pm
Saturday - 7am to 3pm

South Manchester Public Protection Investigation Unit: 0161 8566053 and 0161 8566080
Monday to Saturday – 8am to 4pm

Salford Public Protection Investigation Unit: 0161 856 5171

Monday to Friday – 7am to 6pm

Saturday – 7am to 3pm

Tameside Public Protection Investigation Unit: 0161 856 9363

Monday to Saturday – 8am to 4pm

Stockport Public Protection Investigation Unit: 0161 856 7974

Monday to Sunday – 7am to 5pm

Bolton Public Protection Investigation Unit: 0161 856 5788

Monday to Friday – 8am to 4pm

Saturday to Sunday – 7am to 3pm

Wigan Public Protection Investigation Unit: 0161 856 7954

Monday – Sunday 7am until 8pm

Trafford Public Protection Investigation Unit: 0161 856 7574

Monday – 7am to 4pm

Tuesday to Friday – 7am to 8pm

Saturday and Sunday – 7am to 3pm

Rochdale Public Protection Investigation Unit: 0161 856 8069

Monday to Friday – 7am to 11pm

Saturday and Sunday – 7am to 5pm

Oldham Public Protection Investigation Unit: 0161 856 4551

Monday to Friday - 7am to 9pm

Saturday and Sunday – 7am to 5pm

The Domestic Violence Disclosure Scheme (Clare's Law) gives members of the public a formal mechanism to make enquiries about an individual who they are in a relationship with or who is in a relationship with someone they know where there is concern that the individual may be violent towards their partner. Applications can be made at police stations, by phoning 101 (the non emergency number for the police), or by speaking to a member of the police on the street.

Services Available to Perpetrators of Domestic Violence and Abuse

Respect

The National Association for Domestic Violence Perpetrator Programmes and Associated Support Services

Tel: 020 7549 0578
E-Mail: info@respect.uk.net
Web: http://www.respect.uk.net

Appendix 2

Checklist for Managers: Responsibilities Following A Disclose of Domestic Violence and Abuse

Description	✓
Take care to respond in a sensitive and non-judgmental manner and provide initial support	
Confidentiality	
Agree with the employee who should be informed. Keep all information confidential (subject to the requirements of child and adult safeguarding and except where there is a risk of death or serious injury)	
Safety	
Bear in mind that maintaining safety is crucial. Discuss with the employee whether there is any risk to their safety at home and or at work	
Encourage the employee to seek help and advice from specialist Domestic Violence and Abuse agencies, as detailed in Appendix 1	
If there are concerns about the safety of the employee or any immediate vulnerable family members, contact a member of the Council's Independent Domestic Violence Advice Service for further advice; discuss possible referral to the police. The employee can also phone the police domestic violence officers for advice (contact numbers in Appendix 1)	
Consider making a referral to MARAC by completing the Manchester Domestic Violence and Abuse Referral and Assessment Form from: www.manchester.gov.uk/info/200036/domestic_violence/550/get_help_and_advice_about_domestic_abuse/3	
Consider whether a description of the perpetrator should be shared with security and colleagues	
If there are any concerns about safety at work, contact Health and Safety to seek advice from Health and Safety in carrying out a risk assessment and taking action to minimise risks in the workplace.	
Remind colleagues not to give out details of work appointments, locations etc, which may compromise safety	
Record any incidents of harassment or unwanted contacts at work through the Council's Violent Incident Report Form (includes verbal and physical)	
Consider a review of car parking arrangements for the employee where relevant	
Consider whether there are also children or adults at risk living in the household and seek advice from the Independent Domestic Violence Advice Service.	
Discuss all actions you are taking with the employee and explain the reasons for them.	

Appendix 3

EMPLOYEE DOMESTIC VIOLENCE AND ABUSE

MANAGEMENT MONITORING FORM

This form must be completed by the appropriate manager when instances of Domestic Violence and Abuse are reported to them. After completion, this form must be sent (under Confidential cover) to the Employee Relations Team (HROD).

Directorate:

Section/Office:

Date Manager notified:

Where the Employee is a VICTIM of Domestic Violence and Abuse

Action requested by Employee (if any):

Safety measures put in place (if any):

Employee referred for further support to:

Outcome:

Feedback on the practical application of this policy:

Where Employee is PERPETRATOR of Domestic Violence and Abuse

Management Action taken:

Feedback on the practical application of this policy:

Manager's Name:

Job title:

Date: