CITY OF WOLVERHAMPTON COUNCIL

Response to Request for Information

Reference FOI 002339
Date 25 May 2018

Social Media Policy

Request:

1. Do you have a social media policy for social workers? Note: by social media policy we mean a documented policy which gives advice on what social workers employed by the council/service can and can't use social media for.

   a) Can you attach a copy of the policy?

2. Do you have a general social media policy for all council employees? Note: by social media policy we mean a documented policy which gives advice on what employees can and can't use social media for.

   a) Can you attach a copy of the policy?

In respect of your above questions, it has been established after careful consideration that the Council does not hold the above information as we do not have a specific Policy for Social Workers within Children or Adult Services. However, this is currently being considered by the Wolverhampton Safeguarding Board.

Consequently, we are unable to provide any information relating to the above, and are informing you as required by Section 1(1) (a) of the Act, that states:

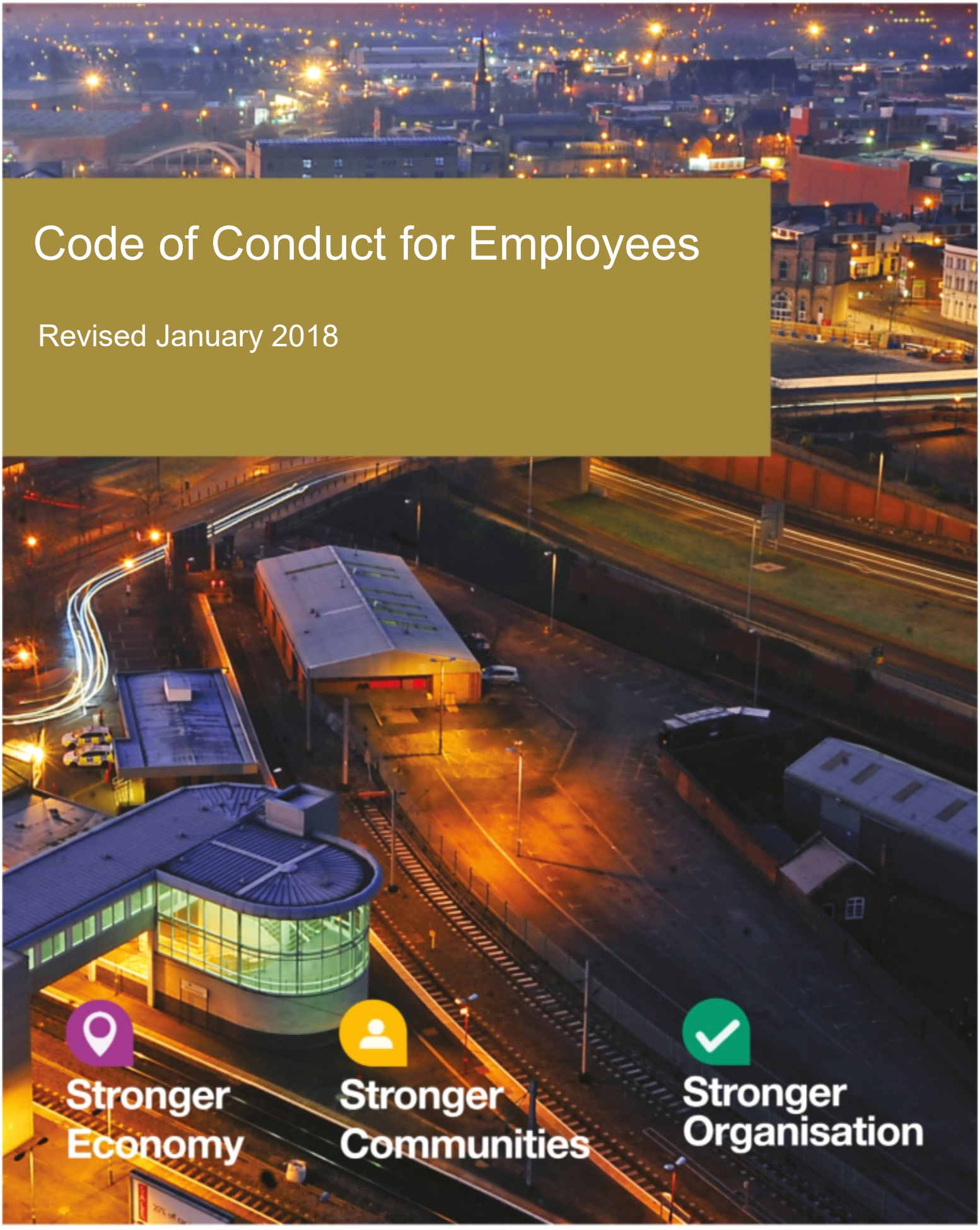
"Any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request".

However, we can inform you that we comply with corporate/HR Policies and have attached the document.

Also, please find attached document which provides our ICT and social media policy. Please note that this is currently under review but is live.

Code of Conduct for Employees

Revised January 2018



wolverhampton.gov.uk

CITY OF WOLVERHAMPTON COUNCIL

INDEX

1. Introduction

1.1 The public is entitled to expect the highest standards of conduct from all employees who work for local government. This Code of Conduct outlines existing laws, regulations and conditions of service to assist employees in their day-to-day work. The Code has been produced in light of the challenges that employees face in a new and more commercially orientated environment.

1.2 The aim of the Code is to lay down guidelines for local government employees which will help maintain and improve standards and protect employees from misunderstanding or criticism.

1.3 Employees must not, either in an official capacity or in any other circumstance, conduct themselves in a manner which could reasonably be regarded as bringing the Council into disrepute.

1.4 Employees who fail to meet the highest standard of conduct will be managed in accordance with the Council's Disciplinary Policy and Procedure.

2. Scope

2.1 The Code applies to all local government employees in Wolverhampton. Inevitably some of the issues covered by the Code will affect senior, managerial and professional employees more than it will others. The Code is intended to cover all employees under a contract of employment within the Council, including office holders such as registrars.

3. Principles

3.1 The Council has five core behaviours that are at the heart of every employee's contract of employment and all work should be undertaken in accordance with these.

PRIDE: our core behaviours

Working as one to serve our city

	How we will behave	
P	**Put customers first -** *be customer focused*	We deliver for our customers, satisfying their needs and empowering employees to do the right thing.
R	**Raise the profile of the City -** *be positive*	We are confident advocates for the city and the council. We are positive about what we do and work actively with our partners to build confidence.
I	**Inspire trust and confidence -** *be open*	We value each other's contribution, empathise with colleagues, are self-aware and remain open in difficult situations. We are flexible and open-minded in our approach. We listen and respond to new ideas.
D	**Demonstrate a can-do and tenacious attitude -** *be a change agent*	We take the initiative, take ownership of problems and see them through, challenging where appropriate and acknowledge uncertainties. Importantly, we will be evidence-led in our decision-making.
E	**Encourage teamwork -** *be a team player*	We work as one council, sharing ideas, each other's priorities and problems. We work together to develop shared, sustainable solutions to complex problems.

4. Standards

4.1 Local government employees are expected to give the highest possible standard of service to the public and where it is part of their duties, to provide appropriate advice to Councillors and fellow employees in an impartial manner. Employees will be expected, through agreed procedures and without fear of recrimination, to bring to the attention of the appropriate level of management any deficiency in the provision of service. Employees must report any impropriety or breach of procedure to the attention of a Senior Manager.

4.2 In carrying out their duties, employees will act with professionalism and will follow the Council's Every Contact Counts customer service standards at all times.

4.3 The Council must maintain the image of a professional public service organisation, providing high quality services. Therefore, all employees must ensure they present a tidy and professional image of the council and present a positive first impression. All employees must ensure that they are appropriately dressed for their duties

4.4 The City of Wolverhampton Council respects the right for employees to adhere to religious and cultural observances, however, employees who wish to make modifications to their uniforms to reflect their beliefs must discuss and agree them with their line manager.

4.5 The council will allow some modification to the uniform for employees with specific medical conditions, however employees who wish to make such

modifications to their uniforms or work attire must agree them with their line manager in conjunction with Corporate Communications.

4.6 Employees who are provided with an access pass or identification card must wear them on a corporate branded lanyard. All employees who have daily, face-to-face contact with our customers must wear a name badge at all times.

4.7 Employees must not wear their uniform, access pass or identification cards when not at work, and are required to return all items on termination of their contract of employment on their last day of work. This is to maintain the integrity of the council's corporate image by minimising the risk of the council being misrepresented. Corporate uniforms, access passes and identification cards must not be made available to non-council employees.

5. Disclosure of Information

5.1 It is accepted that open government is best. The law requires that certain types of information must be made available to Councillors, auditors, government departments, service users and the public. The law also recognises that this information is confidential. Employees should ensure that confidentiality of information is maintained as required by the law and by the Council.

5.2 Employees must not use any information obtained in the course of their employment for personal gain or benefit, nor should they pass information on to others who might use it in such a way, This is also expected and should be applied when employment with the Council has terminated and the person is no longer an employee. Any particular information received by an employee from a Councillor which is personal to that Councillor and does not belong to the Council should not be divulged by the employee without the prior approval of that Councillor, except where such disclosure is required or sanctioned by the law.

5.3 Employees must ensure that they adhere to the Council’s Information Governance Framework and associated policies and procedures at all times.

6. Political Neutrality

6.1 Employees serve the Council as a whole. It follows they must serve all Councillors and not just those of the controlling group, and must also ensure that the individual rights of all Councillors are respected.

6.2 It is recognised in some circumstances that political parties will wish to formulate their policies in private, yet require employee input. Confidentiality should be maintained in these circumstances.

6.3 Employees (whether nor not politically restricted under the provisions of the Local Government and Housing Act l989) must follow every lawful expressed policy of the Council and must not allow their own personal or political opinions to interfere with their work.

6.4 Political assistants appointed in accordance with the Local Government and Housing Act 1989 are exempt from the standards set in paragraphs 6.1 and 6.3.

7. Relationships

7.1 Councillors

Employees are responsible to the Council through its senior managers. For some, their role is to give advice to Councillors and senior managers and all are there to carry out the Council's work. Mutual respect between employees and Councillors is essential to good local government. Close personal familiarity between employees and individual Councillors can damage the relationship and prove embarrassing to other employees and Councillors and should therefore be avoided.

7.2 The Local Community and Service Users

Employees should always remember their responsibilities to the community they serve and ensure that a courteous, efficient and impartial service is delivered to all groups and individuals within that community as defined by the policies of the Council.

Employees should avoid unnecessary personal familiarity with service users and customers that they come into contact with in the course of their work. They should not use their position to either take unfair advantage of members of the public who use Council services or allow themselves to be unduly influenced by them. Employees must ensure their professional integrity is maintained at all times.

7.3 **Contractors**

All relationships of a business or private nature with external contractors, or potential contractors, should be made known to a senior manager. Orders and contracts must be awarded on merit, by fair competition against other tenderers, and no special favour should be shown to businesses run by, for example, friends, partners or relatives in the tendering process. No part of the local community should be discriminated against.

7.4 Employees who engage or supervise contractors or have any other official relationship with contractors and have previously had or currently have a relationship in a private or domestic capacity with contractors, should declare that relationship to their Senior Manager.

7.5 **Spouses, partners and close personal friends**

Employees who have a close personal relationship with any other employee of the Council should take special care to ensure that the relationship does not interfere with normal working relationships and does not cause others to doubt that they will be treated fairly. If it does, appropriate action will be taken in such circumstances.

7.6 People who already have a close personal relationship should not seek employment in the same work group. Senior managers have a particular responsibility to ensure that there can be no question of favouritism or bias in the appointment or treatment of any person with whom they have a close personal relationship outside of their particular work group.

7.7 Where employees are involved in a close personal relationship with a work colleague that has broken down, they must ensure that they do not involve others in their private affairs within the workplace. Relations and/or their breakdown must not interfere with working arrangements.

7.8 Employees who are in, or embark on, a close personal relationship within the same service or department must declare the relationship to their manager and may voluntarily sign the protocol at Appendix 1 to help ensure probity and appropriate behaviours. Dependent on the working arrangements, the nature of the post(s) held and an assessment of the potential risk to the organisation, the relevant Strategic Director/Director/Service Director may require employees to sign the relationship protocol. Signed relationship protocols will be maintained confidentially by the Head of Human Resources and a copy placed on each individual's personal file. Protocol is available on a voluntary basis in cases where staff are engaged in a close personal relationship that is further removed from working in the same department.

8. Appointment and Other Employment Matters

8.1 Employees involved in appointments should ensure that these are made on the basis of merit. It is improper for an employee to make an appointment which was based on anything other than the ability of the candidate to undertake the duties of the post. In order to avoid any possible accusation of bias, employees should not be involved in an appointment where they are related to an applicant, or have a close personal relationship outside work with him or her.

8.2 Similarly, employees should not be involved in decisions relating to discipline, promotion, or pay adjustments for any other employee who is a relative, partner, etc.

9. Outside Commitments

9.1 All employees should be clear about their contractual obligations with the Council and should not take outside employment which conflicts with the Council's interests. Employees should declare to their senior manager any outside commitments that could be considered as having some similarity with their Council duties or might cause conflict.

9.2 The Council retains ownership of intellectual property or copyright created during a person's employment.

10. Personal Interests

10.1 The Director of Governance will maintain a register of employees' interests outside their contract of employment. All employees should, without delay, notify the Director of Governance and their Senior Manager of outside interests which cover:-

(a) Any non-financial interests that they consider could bring about conflict with the Council's interests;

(b) Any financial interests which could conflict with the Council's interests;

(c) Membership of any organisation not open to the public without formal membership and commitment of allegiance and which has secrecy about rules or membership or conduct.

10.2 The register of employees' interests will be kept on a confidential basis.

11. Equality Issues

11.1 All local government employees should ensure that policies relating to equality issues as set down by the Council are complied with in addition to the requirements of the law. All members of the local community, customers and other employees have a right to be treated with fairness and equity.

12. Separation of Roles during Tendering

12.1 Employees involved in the tendering process and or dealing with contractors should be clear on the separation of client and contract roles within the Council. Senior employees who have both a client and contractor responsibility must be aware of the need for accountability and openness.

12.2 Employees in contractor or client units must exercise fairness and impartiality when dealing with all customers, suppliers other contractors and sub-contractors.

12.3 Employees who are privy to confidential information on tenders or costs for either internal or external contractors should not disclose that information to any unauthorised party or organisation.

12.4 Employees contemplating a management buy-out should, as soon as they have formed a definite intent, inform the Managing Director and withdraw from the contract awarding processes.

12.5 Employees should ensure that no special favour is shown to current or recent former employees or their partners, close relatives or associates in awarding contracts to businesses run by them or employing them in a senior or relevant managerial capacity.

13. Corruption

13.1 Employees must be aware that it is a serious criminal offence for them corruptly to receive or give any gift, loan, fee, reward or advantage for doing, or not doing, anything or showing favour, or disfavour, to any person in their official capacity. If an allegation is made it is for the employee to demonstrate that any such rewards have not been corruptly obtained.

14. Use of Financial Resources

14.1 Employees must ensure that they use public funds entrusted to them in a responsible and lawful manner. They should strive to ensure value for money to the local community and to avoid legal challenge to the Council.

15. Hospitality

15.1 Employees should accept offers of hospitality only if there is a genuine need to impart or receive information or represent the Council in the community. Offers to attend purely social or sporting functions should be accepted only when these are part of the life of the community or where the Council should be seen to be represented. They should be properly authorised and recorded.

15.2 When hospitality has to be declined those making the offer should be courteously but firmly informed of the procedures and standards operating within the Council.

15.3 Employees should not accept significant personal gifts from contractors and outside suppliers, although employees can keep insignificant items of token value such as pens, diaries, etc.

15.4 When receiving authorised hospitality employees should be particularly sensitive as to its timing in relation to decisions which the Council may be taking affecting those providing the hospitality.

15.5 Acceptance by employees of hospitality through attendance at relevant conferences and courses is acceptable where it is clear the hospitality is corporate rather than personal, where the Council gives consent in advance and where the Council is satisfied that any purchasing decisions are not compromised. Where visits to inspect equipment, etc. are required, employees should ensure that the Council meets the cost of such visits to avoid jeopardising the integrity of subsequent purchasing decisions.

16. Sponsorship – Giving and Receiving

16.1 Where an outside organisation wishes to sponsor or is seeking to sponsor a local government activity, whether by invitation, tender, negotiation or voluntarily, the basic conventions concerning acceptance of gifts of hospitality apply. Particular care must be taken when dealing with contractors or potential contractors.

16.2 Where the Council wishes to sponsor an event or service neither an employee nor any partner, spouse or relative must benefit from such sponsorship in a direct way without there being full disclosure to a Senior Manager of any

interest. Similarly, where the Council through sponsorship, grant aid, financial or other means, gives support in the community, employees should ensure that impartial advice is given and that there is no conflict of interest involved.

17. Use of Council Assets

17.1 Council assets compromise of not only physical and financial resources but also computer data and information.

17.2 Employees must ensure they have the necessary authorisations and permissions before using council property.

17.3 Employees must ensure they comply with the Council's policy on the Personal Use of ICT and Social Media and the Council's Information Governance Framework.

18. Whistleblowing

18.1 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment employees are encouraged to come forward and voice any serious concerns they may have over any aspect of the Council's work.

18.2 If employees become aware of any activities that are non-compliant with this Code of Conduct, they must report the matter through the Council's Whistleblowing Policy.

18.3 Any employees who raise concerns do so without the fear of victimisation, subsequent discrimination or disadvantage.

19 Liability of Employees

19.1 This section sets out the support which the Council gives to employees if claims are made against them by third parties arising out of alleged acts or defaults whilst they are carrying out their duties and responsibilities as employees of the Council. NB: for the purposes of this policy, any Returning Officer appointed by the Council is covered by the term 'employee' as used hereafter.

19.2 Providing an employee is not acting in a fraudulent or dishonest manner, and is not reckless or grossly negligent, or acting outside the scope or spirit of his or her normal duties, the Council will provide liability cover for any action taken against the employee by third parties arising out of the normal course of

carrying out Council business, including the management of elections or referenda. This cover does not prevent disciplinary action being taken where appropriate and cover cannot be provided for criminal, wilful or reckless acts.

19.3 Claims may arise in a number of ways:

(i) As the result of a direct action by a third party against the employee;

(ii) As a result of the employee being joined in an action by a third party against the Council;

(iii) As a result of a direct action by a third party against the Council.

19.4 The general rule of law is that an employer is liable for the acts or defaults of an employee provided that individual was acting within the scope of his/her employment. This can also extend to the situation where a third party reasonably believes the employee had proper authority to do what he or she has done, even if this is not actually the case.

19.5 It is normal practice in the public and private sectors for employing bodies to indemnify their employees. Employees of City of Wolverhampton Council are covered by a resolution of the Finance and General Purposes Committee dated 13 April 1987:

That the Council shall indemnify in perpetuity all employees and former employees of the Council against all liability, professional or otherwise, for negligence or negligent omission or breach of contractual or statutory duty arising out of the employee's employment with the Council and that such indemnity shall extend to any such liability arising out of the employee's engagement of duties undertaken by the Council on behalf of any other authority or body.

Provided that such indemnity shall not extend to any liability arising as a result of fraud, dishonesty or other criminal activity or of wilful misconduct, gross negligence or gross dereliction of duty on the part of the employee.

19.6 The indemnity will not apply if any employee, without the authority of the Council, admits liability or negotiates or attempts to negotiate a settlement of any claim falling within the scope of this policy.

19.7 Insurance cover relevant to employees is as follows:

- Public and employers' liability
- Officials indemnity (financial loss to third parties)
- Libel and slander
- Cash in transit

- Personal accident (assault)
- Travel cover (on request) for official journeys outside the UK
- No claims bonus and excess protection cover (on request and contributory premiums)

19.8 Where an employee is involved with an external body or company, the situation is more complex and depends on the nature of the role undertaken, whether as an observer, adviser or part of the management of the organisation. This is covered in more detail in the Code of Practice for Service on Outside Bodies, approved by the Audit Committee on 27 February 2006.

19.9 As part of its risk management, the Council sometimes agrees deductibles (an excess) for an insurance policy at a higher level than may be required by the market. The cost of any deductible is met out of the Council's Insurance Fund. In the event that a claim is made against an employee in respect of duties carried out in the course of his or her employment, the Council will indemnify the employee against the cost of any deductible that may fall due, subject to the provisions outlined above.

20. Supporting Regulations, Codes and Procedures

20.1 Supporting this general Code of Conduct are specified detailed regulations and procedure codes:

Contracts Procedure Rule

Financial Procedure Rules

Anti-Fraud and Corruption Policy

Anti-Money Laundering Policy

Whistle Blowing Policy

Hospitality Code

Human Resources policies and procedures

National Scheme of Conditions of Service

Equal Opportunities Policy

Computer Security Policy

Service Group Instructions and Codes

APPENDIX 1

CLOSE PERSONAL FRIENDSHIP PROTOCOL

Names: _____

INTRODUCTIONS

The following protocol has been agreed between the above parties to ensure probity between _____ and _____. The protocol is to protect the integrity of both parties, ensure probity and transparency and avoid allegations of favouritism or inappropriate decision making. This is a protective document and does not suggest any impropriety by the signing partners whatsoever.

EXCLUSIONS

This protocol does not remove the right of the Council to respond to any formal complaints received by the Managing Director, Monitoring Officer or Head of Human Resources with an investigation if this is deemed necessary or appropriate by the Managing Director.

PROTOCOL

Line Management

1. [The arrangements for line management will be explained here].

Operational Management Activities

2. Neither party to this protocol will sign or countersign the following in relation to the other party in this protocol:

   (a) Travel Claims
   (b) Subsistence Claims
   (c) Training or development activities
   (d) Attendance at conferences
   (e) Changes to ICT equipment or telephone
   (f) Appraisal or other performance processes
   (g) Annual leave
   (h) Purchase of new equipment
   (i) Procurement of goods or services by a third party initiated by the other party in this protocol

Promotion or Alternative Work

3. Neither party to this protocol will sign, countersign, instigate or suggest to any third party the following:

   (a) Promotion within the current work area
   (b) Promotion to another part of the Council
   (c) Secondment to another area within the Council
   (d) Salary changes of any description
   (e) Regrading
   (f) Honorarium Payments
   (g) Additional payments of any kind

Confidential Information

4. Both parties to this protocol agree that they will not share confidential information of any nature and will not reveal to each other any information about the other's employment with City of Wolverhampton Council.

Interview Panels and Recruitment Processes

5. Neither party to this protocol will be involved in an interview panel or recruitment process involving the other or jointly sit on any interview panel.

Disciplinary or Redundancy or other matters

6. Neither party to this protocol will be involved in processes which involve the other party unless specifically requested to do so by the Managing Director, (or Investigating Officer in the case of a disciplinary investigation).

Spirit of the Protocol

7. Where something is not specifically referred to in this protocol it is agreed that the spirit of the protocol will be observed.

Close Friendship

8. Should the close friendship cease to be so the protocol will remain in force until City of Wolverhampton Council no longer employs one of the parties.

Both Parties to the Protocol Note

9. Both parties note that this protocol is purely precautionary to protect both parties from unfounded or inappropriate suggestions of favouritism or misconduct at City of Wolverhampton Council.

The following parties have signed the protocol and will ensure adherence to it:

Name:	Name:
Position:	Position:
City of Wolverhampton Council	City of Wolverhampton Council

Copies of this protocol are distributed as follows:

1.
2.
3.
4.

Wolverhampton City Council

Human Resources Policy Framework

Policy on Personal Use of Council Computer Equipment, and Access to Social Media

Approved by:	*Cabinet Resources Panel (26.06.2013)*
Published:	*01.07.2013*
Review date:	*01.07.2014*

CONSULTATION		
The following officers and or bodies have been consulted on this policy:		
Officers and or Bodies	From	To
Andy Hoare	01.07.2012	01.07.2013
Alistair Merrick	0.07.2012	01.07.2013
HR	04.02.2013	08.02.2013
CDB/SEB	13.06.2013	
MRG	06. 2013	
CCC Scrutiny Panel	20.06.2013	
The following Trade Unions have been consulted on this policy		
	From	To
Unison	06.2013	07.2013
GMB	06.2013	07.2013
Unite	06.2013	07.2013

REVIEW LOG			
Date	**Version**	**Comments/Review**	**Approved by**
22.01.13	0.1	GW following review by AH & AM	

EQUALITY ANALYSIS
An equality analysis is being carried out on this policy and procedure. Contact HR Strategy and Policy Team for a copy. Contact HR on 01902 552345 or by email on ***HR.supportdesk@wolverhampton.gov.uk*** *for HR advice.*

ADVICE
Contact HR on 01902 552345 or email ***HR.supportdesk@wolverhampton.gov.uk*** for HR advice.

COMMENTS AND AMENDMENTS
Contact HR on 01902 552345 or email ***HR.supportdesk@wolverhampton.gov.uk*** to make any comments or suggest any feedback on this policy.

DISTRIBUTION
This policy and procedure is placed on the HR intranet for managers and employees to view. Copies will be provided to recognised Trade Unions and managers electronically.

INDEX

1. Policy Statement

1.1. The Council's policy on personal use of Council computer equipment and access to social media sets out the standards and expectations of acceptable use for employees. Acceptable use, as set out in this document, includes measures to manage the personal and organisational risks associated with use of ICT resources and digital media services.

1.2. The policy includes:

- information on when you are and are not allowed to use Council computer equipment for personal activities
- risks and other issues you should be aware of when using Council computer equipment for personal activities
- rules and guidelines for using online services such as social media sites and collaboration services.

1.3 Abuse of the permissions in this policy or breaches of its provisions will be dealt with under the Council's disciplinary policy and procedures.

1.4 It is important that all employees understand this policy. Allowing you to use Council computer equipment for personal activities exposes the Council's ICT systems and information to increased risks. Ultimately this is a risk to members of the public as well, especially where personal information is involved. You are expected to use this privilege thoughtfully; to follow advice and guidance; and to accept responsibility for your own activities.

1.5 By using Council-supplied computer equipment or logging on to the Council's computer network you are confirming that you are aware of this policy, you understand it, you accept its provisions, and you agree to abide by it.

1.6 Wherever Council services such as email are mentioned in this policy, the same rules or guidance also applies to any similar service (such as GCSX/GCF secure email).

1.7 This policy applies anywhere employees use Council ICT services (so, not only in the office, but also connecting from home or out "on the road").

1.8 This policy is about matters that are changing rapidly. The policy may be amended at any time to respond to emerging issues and opportunities.

1.9 The Council is obliged to comply with a range of regulations that affect the way its ICT and information resources may be used. This policy does not override those regulations. You should be aware of them and take them into account when you use Council ICT equipment or services, whether for professional or for personal use.

2. Scope

2.1 This Policy and Procedure applies to all employees of the Council including Chief Officers and employees based in schools. It also applies to Councillors.

3. Restrictions

3.1 When you are logged on to the Council's network there a few basic things that you are routinely prevented from doing:

- Accessing Council software and information that you are not authorised to use.[1]
- Accessing certain kinds of Internet sites and services, such as:
    - Those believed to contain inappropriate material.[2]
    - Those believed to pose a serious threat to the security of the Council's network, data and systems.[3]
    - Those believed to use technologies that can hamper the performance of the Council's network and systems, and prevent colleagues from carrying out their duties effectively.[4]

3.2 Like other organisations, the Council uses commercial "web site reputation" services to decide which Internet sites should be blocked. The nature of the Internet makes it impossible for such services to be perfect.[5] Therefore contact the ICTS Service Desk if:

- You are unable to access something that you think you should be able to access.
- You find that you are able to access an inappropriate site.
- You receive security warnings when trying to access a site. **In this case, do not take any further action, including clicking buttons, until you have been advised by ICTS.[6]**

3.3 ICTS monitors the security and performance of the network and other computer resources, and may intervene without notice to protect them. This may result in temporary or permanent loss of services you have used previously.

---

[1] E.g. only staff with appropriate authorisation can use business software such as systems for Social Care, Benefits, Finance, Environmental Services, and so on.
[2] E.g. pornography, hacking, illegal file-sharing, etc.
[3] E.g. from viruses, bots and other malware.
[4] E.g. certain kinds of "streaming media" such as videos.
[5] Reputation services monitor web sites and categorise them according to their content (e.g. "government", "sport", "shopping" etc). ICTS then blocks access to specific categories according to agreed corporate policy. The Web is such a big and dynamic place that sites can be put into the wrong category by the reputation service. Individual sites may be unblocked by request regardless of their category.
[6] Security warnings can be fakes. By clicking a button to "fix" the alleged problem you may actually install a virus or malware on the PC.

3.4 By default, you are not prevented from using Internet sites and services such as shopping and popular social media services. Your use of these is subject to the principles and guidelines set out later in this policy.

4 Permissions: Principles And Guidelines

4.1 At your manager's discretion, you may make reasonable use of Council computer resources for personal activities on the Internet. This includes social media[7] and shopping.

4.2 The Council expects you to use this privilege responsibly. It exposes the Council, members of the public, and you, to direct and indirect risk. You may be liable for the consequences of misuse, whether deliberate or accidental. If you are unsure about any activity, seek advice before you do it.

4.3 Personal use is not a right. Your manager may choose not to allow it. Your Head of Service may ask ICTS to block web sites that are available by default to colleagues elsewhere in the Council.

4.4 You should limit your personal use to non-working hours of your day. If you are on flexi-time, you should be clocked out.

4.5 You may only use Council equipment for personal activities if the device is attached to the corporate network by cable or wi-fi. Do not use smartphones (including Blackberries and Palm PDAs) or laptop dongles to access the Internet unless it is for Council business. These devices connect via commercial mobile networks for which the Council has to pay according to the amount of data transmitted.

4.6 If you use social media sites for official Council business, you should have agreed an appropriate way of using them with your manager. You or your manager should consult the Council's Marketing and Communications Team for guidance on any public-facing use of social media; whether informal, or as part of service delivery, or as part of a publicity campaign.

4.7 Unless you are authorised to do so, avoid engaging with members of the public about Council-related matters via social media. If you publish comments, do not convey the impression that you are speaking on behalf of the Council unless that is part of your job. It is very easy for your personal and professional identities to become mixed up online and it is important that you are alert to the risks from this.[8]

4.8 You must not disclose information about the Council or members of the public unless you have authority to do so. You should consider the impact of

[7] E.g. Facebook, Twitter, Google+, LinkedIn, Flickr, Yammer etc.
[8] The Council's Marketing and Communications Team provide more detailed guidelines on the use of social media and the boundary between professional and personal use.

releasing any kind of information (whether intentionally or accidentally) and you may be liable for any consequences if you do.

4.9 If you use social media such as blogs and Twitter to comment on aspects of your professional life[9] you should consider the way your words might be understood and used by other people. This is especially important if you can be identified as an employee of Wolverhampton City Council, which is often easy to do even if you are using a fake identity online. This applies even if you write in your own time away from the office. If in any doubt, seek advice before publishing.

4.10 Access to webmail services such as Google Mail, Hotmail and Yahoo is not allowed. These services will remain blocked. Viruses and malware are often transmitted as attachments to email messages. In normal email, these are detected by the Council's anti-virus systems before they reach your Inbox. With webmail such attachments cannot be scanned by the anti-virus system[10] and they pose a very serious threat to the Council's systems.

4.11 You are allowed to use your Council email address for moderate personal activities, such as social communications. **If you choose to do this, bear in mind that the Council cannot guarantee that the content of your emails will remain private**. Ensure that you have read and understand the **ICT Services Statement on Employee Privacy** (Appendix 1).

4.12 Do not use your Council email address if you register for services or buy personal goods online. You may use your Council email address to register for professional services, such as appropriate news alerts and professional forums[11] and membership of professional bodies.

4.13 Avoid using the same online accounts for both personal and professional activities. There are some circumstances in which separate accounts can be difficult[12]; in this case consult the Council's Marketing and Communications Team.

[9] Whether your own activities or those of others, or the work of the Council, or government and politics in general.
[10] When accessing webmail your messages are displayed over an encrypted connection. The Council's anti-virus systems are unable to decrypt such messages to scan them.
[11] E.g. The LGA Knowledge Hub or forums operated by professional bodies.
[12] E.g. Some social media sites require that you register as an identifiable person, rather than sharing a business identity.

5 Risks

5.1 Allowing access to online services greatly increases the risks that the Council has to deal with, and you should use them with appropriate caution. Directly or indirectly, it is possible to cause harm to the Council, or to members of the public, or to yourself.[13] You may be liable for the consequences of misuse, whether deliberate or accidental.

5.2 A common way to spread viruses and malware is to get you to click on a link to a booby-trapped web page or web program. Often this is done via emails or Twitter messages. Take care when following any link, including those in personal webmail messages, because any damage will be caused to the Council's systems, not to your personal account.

5.3 Rogue links are often disguised as something plausible from banks or online services, or they may use "URL shortening" services.[14] The latter are now very popular on Twitter and elsewhere and are often used legitimately. Unfortunately there is currently no reliable way of telling legitimate from rogue links, so unless you are confident that the link has been sent by a safe source you should not click on it.

5.4 Many web sites and online services use special technologies to enhance your experience when using them.[15] These technologies run programs on your PC or smartphone and there is nothing to tell you reliably what they are doing:

- Never download "apps" or other programs and try to install them on a Council device
- If a web site says you must install an add-on to make the site work, do not proceed
- ICTS disables many such technologies by default. As a result, sites and services that work for you on your home PC may not work properly on Council devices
- ICTS will not offer support for web sites and online services that you are using for personal activities.

5.5 Streaming media[16] are particularly heavy users of resources such as the Council's connection to the Internet, and the internal network that connects to your PC. If possible avoid displaying web pages that use streaming media; and if you do display one, close the browser as soon as possible after you have seen what you need to see. Do not simply minimise the browser or open another tab, because the video may continue to use resources in the background.

[13] This can happen if confidential information is made available outside the Council, or if viruses or malware are introduced to the Council's network or systems, or if online services takes up excessive amounts of ICT resource (such as bandwidth of the corporate connection to the Internet).
[14] Such as Tinyurl.com, Bit.Ly and T.co.
[15] Examples of such technologies include "apps", extensions, add-ons, toolbars, buttons and scripts.
[16] "Streaming media" are video or audio that is played continuously in real time from a web site such as the BBC or YouTube.

5.6 It is tempting to visit sites with streaming media to follow events such as sports. Each member of staff that gives in to this temptation adds to the load on the Council's network and lowers its capacity for handling real work. ICTS may intervene to block such sites without warning if there is cause for concern. Bear in mind that you should only carry out personal activities on Council equipment outside your working times.

5.7 Some web sites carry malware that displays a plausible but fake security alert message, which tells you to click a button to scan your PC. Sometimes this may look like a Microsoft message. Clicking any button is likely to install malware on your PC. **If you see such a message contact the ICTS Service Desk by phone to ask for assistance.**

5.8 Do not upload Council documents to file-sharing or collaboration services[17] unless:

- You understand the terms and conditions of using the service, including how your information is used by the service provider and the legal liabilities for disclosure of information;
- You are completely confident that the material you are uploading is appropriate for release to the public domain, even if releasing it is not your intention;
- You know which country the information would be stored in, and the location is compliant with relevant UK and EU legislation;
- You know for sure that you can permanently delete the material from the service[18].

5.9 It is tempting to use such services because they are easy to sign up to and appear to be free of cost. They are not free: they depend on exploiting information you give them.

5.10 Some public sector bodies are now using services such as Google Apps. These are paid-for versions of the service, with security accreditation[19], and contracts that define obligations and liabilities for all parties and specify that the data must be stored in a country that complies with EU legislation.[20] "Free" accounts do not come with these assurances. Publicity can give the impression that because an organisation is using a service, it must be safe for you to use, which may not be true.

[17] E.g. Google Docs, Dropbox, Yammer or any Internet "cloud" platforms.
[18] Many "free" services retain your information even if you close your account. In some cases a facility for deletion is included in paid-for accounts.
[19] Often using special computer data centres built specifically to comply with government security regulations.
[20] Storing information about a person outside the EU may contravene the Data Protection Act. Also, some countries (including the USA) have local laws that give their government agencies the right to look at information stored there even if it belongs to people in other countries. With "free" accounts you almost never have any say about where information is stored.

5.11 Yammer, LinkedIn and similar services are aimed at professionals and may give the impression of greater security. You should treat these services with as much caution as other "free" services. In particular you should be aware that such services often try to copy your contacts list from Outlook or your phone, in which case you might disclose information about other people.

5.12 File-sharing sites are often associated with activities such as distributing illegal copies of copyright material. Do not use such sites even if your material is legal to distribute, because the Council's reputation can be damaged by association.

5.13 Be aware of copyright and licence issues. Just because people publish text and images on the Internet this does not give you an automatic right to copy or reuse them, whether for professional or private purposes.[21] Software or services that are free for personal home use may not be free for professional or corporate use. The Council may be liable if you breach copyright or licence terms.

6 Personal Privacy And Safety When Using Council ICT Resources

6.1 Your personal privacy cannot be guaranteed when you use Council ICT resources. This applies whether your activities are personal or professional. The Council accepts no liability for any consequences if you choose to input information for personal activities.[22] Any personal use of Council ICT resources is at your own risk. **You are advised to treat Council ICT resources with the same caution that you would use on an unsecured public PC, such as in an Internet Café.**

6.2 Ensure that you have read and understand the **ICT Services Statement On Employee Privacy**.

6.3 You should bear in mind that there are risks to members of the public as well as to you and the Council.

- If malware infects the Council's systems and leaks information to the outside world, confidential data about individuals could be disclosed.
- Malware and virus infections or excessive personal use can affect the performance of the Council's systems. This in turn is likely to hamper the delivery of many of the Council's services to the public.

[21] Many web sites and social media services carry copyright or licence statements. For example, images on Flickr may be tagged with a "Creative Commons" licence with various provisions. In some cases these may give you the right to reuse the material, usually subject to limitations and typically requiring you to state whose image it is and where it came from.

[22] Personal information you supply for Council operational purposes (e.g. HR information needed for your employment) will be stored and used in accordance with the Data Protection Act.

7. Roles and Responsibilities

Roles and Responsibilities of Employees

7.1 All employees have a responsibility to comply with all standards, codes and protocols which govern conduct and behaviour including the ICT protocol for the use of Council computer equipment and access to social media. Failure to comply with this policy will be treated as a disciplinary issue.

7.2 Employees are expected to read and understand this policy and to speak to their manager before using any computer equipment or services if there are any issues they are not sure about.

7.3 Employees should use the permissions thoughtfully, follow the advice and guidance given and accept responsibility for their own activities.

7.4 Appropriate authorisations as set out in this policy should be sought for the use of council ICT resources and access to social media.

Roles and Responsibilities of Managers

7.5 Managers have a responsibility to ensure that their staff are aware of this Policy, understand it, accept its provisions and abide by it, and that sanctions can be imposed for breaches of it.

7.6 Managers should advise employees on acceptable use if they have queries.

8. Monitoring and Review

8.1 This policy and procedure will reviewed and updated annually and be available to managers and employees via the HR intranet.

9. Links to other Policies and Procedures

9.1 This Policy is closely linked with the following policies:

- Disciplinary Policy
- Information Government Policy
- Equality Policy

10. Equality

10.1 An Equality Analysis will be carried out on this policy and procedure.

10.2 If any aspect of the Policy on Personal Use of Council Computer Equipment and Access to Social Media causes you difficulty on account of any disability that you may have, or if you need assistance because English is not your first language, you should raise this issue with HR, who will make appropriate arrangements.

.

APPENDIX 1

ICT Services Statement on Employee Privacy

1. About this Document

1.1 This Statement sets out the position and policy of ICT Services (ICTS) regarding the privacy of Wolverhampton City Council (WCC) employees and Councillors who use computer, phone and other ICT resources that are provided by ICT Services.

1.2 It outlines what employees and Councillors may expect when they use corporate ICT resources. The Council's Constitution and Human Resources (HR) policies set out the general principles of employee privacy. In particular those policies address issues relating to personal information, to compliance with the Data Protection Act, and to monitoring of employees' activities. This ICTS Statement complements those principles and does not over-ride or replace them.

2. Acceptance

2.1 If you use WCC ICT resources, including phones, you are confirming that you understand this Statement and accept the policy on privacy that it sets out. If there is anything that you are not sure about, you should seek advice from your manager or Member Services (for Councillors).

2.2 If you manage employees or support Councillors it is your responsibility to make sure that anyone who uses Council provided ICT resources understands and accepts this Statement.

3. Your Privacy When Using Council ICT Resources

3.1 Your personal privacy cannot be guaranteed when you use Council ICT resources. This applies whether your activities are personal or professional. The Council accepts no liability for any consequences if you choose to input information for personal activities.[23] Any personal use of Council ICT resources is at your own risk. **You are advised to treat Council ICT resources with the same caution that you would use on an unsecured public PC, such as in an Internet Café**.

3.2 By default your activities will not be actively individually monitored. This includes the content of emails. But you should note the following:

a) ICTS may intervene to address problems with Council ICT resources. Depending on the nature of the problem it may be impossible to avoid information being seen.

b) Anti-virus software scans every file you open on your PC. These could include personal emails, and any attachments in emails

c) Emails going in and out of the Council are scanned by automated systems to detect the message (including its contents) may be inspected by authorised ICTS

[23] Personal information you supply for Council operational purposes (e.g. HR information needed for your employment) will be stored and used in accordance with the Data Protection Act.

d) staff in the first instance and the possibly other authorised individuals, depending on the nature of the material.

e) In exceptional circumstances, such as suspected illegal activity or severe breaches of discipline, monitoring of an individual's activities (including access to the content of documents, emails and other electronic files) may be authorised by a Strategic Director or Assistant Director of the Council. Data from monitoring will be collected by ICTS and only made available to an independent investigating officer, until it has been established that there is a case to answer.

f) You should always remember that email is insecure by its nature. This is true for email within the Council[24] as well as out on the Internet. If you wish to communicate sensitive or personal information to someone else in the Council[25] you are strongly advised to speak face-to-face or use some other more private means, if possible. Your personal privacy in emails cannot be guaranteed even when sent and received within the Council. The Council will accept no liability for disclosure of any personal information you choose to put in an email, even if the email is not sent outside the Council.

g) You are advised not to use your Council email address for personal commercial transactions (such as online shopping). Information about your transactions may become accessible to other Council employees. **If you use your Council email address, you do so at your own risk**.

h) If you use Council email for moderate social communications, be aware that you might be making information about your relatives or friends accessible to other Council employees.

i) Emails cannot be sent anonymously, whether inside or outside the Council. They are always traceable to the sender's email address and to the logonid used.

j) If you delete an email from your Inbox or other folders in Outlook, a copy may still exist in archives or system backups. This may also be true of emails that are moved automatically from your Inbox based on dates.[26] Even though you cannot see these copies, they are still subject to Freedom of Information, Data Protection and other legal obligations, and ICTS may be asked to recover them for inspection or disclosure.

k) You must not save any personal data to Council devices. Doing this may make the Council liable for Data Protection, Freedom of Information or other statutory obligations relating to your data.

[24] "Within the Council" means any email addresses ending "@wolverhampton.gov.uk" or "@wolverhampton.gsi.gov.uk". For these purposes, Wolverhampton Homes, West Midlands Pension Fund, and Trade Union branch officers should also be assumed to be within the Council.
[25] E.g. HR, Payroll, Occupational Health, Trade Unions, West Midlands Pension Fund, "whistleblowing" contacts.
[26] Corporate information retention periods are awaiting review. For some business teams in the Council, retention periods may be specified by law. Retention periods across the Council are overseen by the Corporate Information Governance Board.

l) Your personal data may be accessible to other staff who know where to look on the PC and on the Council's network. You are especially vulnerable if you share a PC with colleagues, even though you have separate logonids. ICT support staff may also be able to see your data.

m) Do not store your logonids and passwords on your Council PC or smartphone.

n) Do not use the browser's facilities to store personal logonids and passwords, or to pre-fill online forms.

o) Do not tick options to "keep me logged in" at web sites where you have personal accounts. These options are often ticked by default when you go to the web sites, so you may need to un-tick them.

p) When you leave employment by the Council, all data stored in your Council ICT account (including emails and documents) will be made available to your line manager and possibly to other Council employees. It is in your interests to ensure that you delete any data you consider personal.

q) If you are away from the office and an important business issue arises that depends on information in your Council ICT account (including emails), your manager might request access to your account to find the information. To reduce the risk of this you should ensure that you have made appropriate arrangements with your manager for cover during extended periods of absence.[27]

3.3 In addition to the above, any ICT activity may be recorded passively. This is data that ICT systems routinely accumulate as a by-product of any action or event, in logs, caches, web histories, browser cookies, most-recently-used lists, search indexes, audit records, and so on. The corporate ICT infrastructure also logs things that are happening to maintain performance and diagnose problems.

a) Accumulating this data is automatic on all devices and is not aimed at any individual.

b) In many cases the usefulness of your PC or your software would be seriously reduced if it were suppressed.

c) In the event of a problem, the logs and other passively-collected data may be collated and linked to trace the source of the problem. This could result in your activities being identified.

d) Bills from mobile phone providers are itemised, so there is a record of any use you might make of mobile phones, smartphones (including Blackberries and Palm PDAs) and dongles for laptops. This includes data activities such as accessing the Internet and email services.

.

[27] Microsoft Outlook allows you to delegate access to your email to other Council employees, temporarily or permanently. This offers you a limited amount of control over what the other people can see and do with your email. If you want to know more about this facility, contact your team's ICT Coordinator or the ICTS Service Desk.