AGENDA ITEM NO.5

BRISTOL CITY Council

HUMAN RESOURCES COMMITTEE

For Resolution

2nd September 2010

Report of: Strategic Director: Resources

Title: Web Access for Staff / Amendments to the Code of Conduct

Officer Presenting Report: Mark Williams, Corporate HR Manager
Karen Stephens, HR Adviser (Strategic)

Contact Telephone Number: 0117 92 24838/22165

RECOMMENDATION

That the Committee:

(i) notes the decision made by the Strategic Leadership Team with respect to Internet access by staff and monitoring arrangements, including the review of web access, to be carried out by Strategic Directors as below;
(ii) approves the proposed additions to the Code of Conduct for employees, effective from 1st October 2010.
(iii) notes that the Schools Code of Conduct will be the subject of further consultation, and a report to this Committee.
(iv) notes that Strategic Directors will review existing access around "special cases" and "business categories", as stated below.

Summary

The Strategic Leadership Team (SLT) requested a joint report from ICT, HR, Communications and Audit with regard to increasing staff access to web sites, including blogs and social networking sites. A report detailing the case for widening access with associated risks and monitoring arrangements was approved by SLT on 6 July 2010.

These proposals have necessitated an updating of the Code of Conduct for Officers (See Appendix A attached). In addition this report also incorporates a Use of School Communication Systems, covering locally managed schools.

The significant issues in the report are:

SLT approved the case for increasing staff access to web sites, including blogs and social networking sites. Whilst there are clear business benefits in widening web access, there is a risk of increased personal use by staff during working hours. This risk has been highlighted by the Council's Chief Auditor.

It is the responsibility of line managers to actively promote appropriate usage of the Council's information systems and to deal with employees who fail to comply with requirements of the code of conduct. This can include formal action taken under the Disciplinary Procedure.

In 'harmonising' the Council's web access protocols, SLT agreed that Strategic Directors should review existing access to determine those managers/staff who fall within 'Special Cases' and 'Business Plus' categories, as set out below.

The Code of Conduct has been strengthened to provide clear expectations of employees in relation to social networking sites, personal web sites and blogs (see Appendix A below). Members' approval of these changes is requested.

1. Policy

1.1 A Code of Conduct for Employees is in place for all City Council employees. (A separate version applies to employees in locally managed schools). The Code details amongst other things, the Council's policy with respect to employees use of Council property, facilities and equipment and monitoring arrangements. The Code clearly states that email and Internet facilities may be used for personal reasons unrelated to Council business and that such use should be brief, outside of working hours and exclude activities listed under misuse.

1.2 Additions to the Code of Conduct specifically in relation to social networking sites, personal web sites and blogs have been proposed in view of SLT's decision to widen staff access to the Internet (see

appendices). These additions have been undertaken in conjunction with advice from the Council's Data Protection Officer, the Chief Auditor, the Council's legal department, and are in line with the Information Commissioner's Code of Practice.

2. Consultation

2.1 Internal

Revised monitoring arrangements were discussed with Trade Unions at the Policy meeting on 26 March 2010 and further meetings with nominated TU representatives were held on 13 April and 29 June. This matter, together with proposed additions to the Council's Code of Conduct for Employees, was discussed with Trade's Unions at the Policy meeting on 16 July 2010.

A meeting with nominated Trade Unions representatives and ICT and HR to review the output of the 'Netsweeper' monitoring and Code of Conduct changes, was held on 27 July, with further discussion at the TU policy meeting on 9 August 2010.

At the Trade Union meeting on 9 August the amendments to the Code of Conduct were agreed. The Trade Unions requested a period of further consultation before finalising the Schools Code of Conduct amendments, and this was agreed by officers.

In respect of monitoring the use of information systems, the Trade Unions consider that this is a line manager's responsibility, and that the cost benefits of IT monitoring systems that produce reports, need to be quantified and balanced against the risks of misuse.

2.2 External

The amendments to the Code of Conduct reflect the statutory guidance of the Information Commissioner on monitoring employee use of information systems.

3. Context

3.1 SLT has widened staff access to web sites such as blogs and social media in view of perceived business benefits. For example, to allow employees to contribute to web forums such as the Ask Bristol consultation.

3.2 In this context, the joint working group composed of representatives from Corporate Communications, ICT, Strategic HR and Audit considered the following:-

(a) The case for widening access to web sites

There is a balance to be struck between the positive benefits to the business of having access to useful external web sites, and the risk that excessive use by staff might be a waste of resources, or damage the Council's reputation. As use of external sites such as blogs and video sites for legitimate business use has grown, the Council's position needs to be re-evaluated.

The Council itself has created sites that its own staff cannot access. Examples of these include AskBristol consultations, the Leader's video podcast and our own Twitter feed. This is clearly inefficient.

Many of these services are free or low cost to build and operate, and make it comparatively easy for staff to build and maintain information, often not requiring ICT assistance or expensive external contractors. There are significant costs savings possible.

With the growth in partnership-working, use of external sites makes access to information by staff working in different organisations much easier, compared to trying to host information on one partner site.

We do not currently have the capacity within the Council to easily host blogs, collaborative work sites or video. Therefore, these external sites are often the only way to do the work.

These sites are an increasingly useful business tool for sharing best practice, dynamically consulting the public, partnership working and training.

(b) HR Policies and monitoring arrangements

The Code of Conduct for Employees clearly states that email and Internet facilities may be used for personal reasons unrelated to Council business and that such use should be brief, outside of working hours and exclude activities listed under misuse.

A monitoring system was agreed in March 2010, whereby ICT will run a report each month in order to identify the 20 staff with the highest level of Internet usage and undertake some preliminary screening checks. At this stage ICT will advise the employee's line manager, who would be given a contact name within ICT for the purposes of interpreting, and talking through the implications of the data e.g. what this does/doesn't state about their Internet usage. It may be that all usage is work related, in which case no further action is required. If, following this, the manager considers there has been a breach of policy they would take appropriate action in line with BCC policies, taking advice as required from HR, STS and ICT. This approach will be reviewed as reports from the new 'Netsweeper' package are generated. Arrangements for

automated reporting are still under development.

(c) Concerns about misuse and risk assessment

Whilst it is possible to outline a strong case for how these sites can help the Council with its work there are also legitimate concerns about possible misuse by staff, and to date Bristol City Council has not known the extent of any problem, as no routine monitoring is undertaken. Internal Audit completed an audit review of this area in November 2009 (Internet Usage management). This concluded that there was a risk of misuse, with a high impact. This matter was reported to SLT (late 2009) highlighting the need to provide managers with regular monitoring information to enable 'misuse' to be identified and addressed. It was envisaged that such monitoring would also increase the deterrent to misuse.

(d) ICT capabilities for web access monitoring

The City Council has new software in place for filtering web use called Netsweeper. The software can show which websites have been accessed and over what period, but this may not reflect the user's actual behaviour. For instance, many people open a website first thing in the morning and leave it open in the background whilst looking at, and working, on something else.

3.3 The above considerations are submitted for Members' information.

4. Proposal

4.1 SLT agreed that there will be three categories of web access:

(A) Basic Business - which will be extended to include Journals and Blogs and Social Networking (categories that were previously only available with Business Plus access).

(B) Business Plus - which gives access to additional sites such as drug and alcohol abuse sites, entertainment sites etc.

(C) Special cases - content only available to small numbers of staff who make a business case to their Strategic Director

4.2 SLT agreed that Service Directors will review existing access arrangements as necessary to determine those managers/staff who fall within 'special cases' and 'business plus' categories.

4.3 It remains the responsibility of line managers to actively manage appropriate use of the Council's information systems and to deal with any misuse in accordance with the Code of Conduct. The HR Shared Services Centre provides advice to managers on dealing with potential breaches of the Code of Conduct. In addition, ICT will provide specialist advice and information on usage of particular web sites etc to HR in respect of a particular case. Automated reporting for the highest Internet users is still under development, however, the Council has in place web filtering software which prevents employee access to web sites which contain:-

- adult images
- auctions
- criminal skills
- gambling
- games
- hate speech
- humour
- live TV
- match making
- pornography
- profanity
- viruses
- weapons

4.4 The proposed amendments to the Code of Conduct are as set out in Appendix A attached. Members' approval is requested.

5. Other Options Considered

5.1 SLT considered the business benefits of increasing web access for staff, together with identified risks, before making the decision to increase Internet access. They requested that ICT take appropriate action to ensure sufficiently robust web monitoring is put into place.

5.2 Internal Audit is of the view that there remains a high risk of misuse, even after mitigation, and recommends that the risk assessment is reviewed on a regular basis, and that additional mitigation is sought. The Chief Internal Auditor has been asked to attend this meeting for consideration of this report.

6. Risk Assessment

6.1 ICT can report on individual staff use of web sites but it cannot say with certainty how long people spend on the sites. There are significant resource implications for any monitoring undertaken. In some cases monitoring evidence alone will not support a case for Internet misuse. The risk assessment prepared for SLT outlining existing and possible mitigation is attached.

6.2 A separate risk assessment will be conducted for any changes to the Schools version of the Code of Conduct.

7. Equalities Impact Assessment

7.1 Not required as the proposed changes constitute minimal additions to the Code of Conduct for Employees. In addition, the changes to the Code reflect the statutory guidance of the Information Commissioner.

Legal and Resource Implications

Legal

The Report details amendments to the Code of Conduct for Employees. The amendments have been drafted in accordance with legal advice. The Council is under an obligation to ensure employees are made aware of the amendments to the Code.

Advice from Husinara Jones for Head of Legal Services

Financial

(a) Revenue: **}** not sought
(b) Capital: **}**

Land

Not applicable.

Personnel

HR issues are detailed within paragraphs 4.1 to 4.4 above, and in

Appendix A attached.

Appendices

Appendix A -	Proposed amendments to the Code of Conduct for Employees (BCC)
Appendix B -	Risk assessment prepared for SLT

LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985
Background Papers:

None

Appendix (5) A

Code of Conduct - Amended extract

11.1 **Personal Use**

Employees should note that the Council's property and facilities are provided for official Council business.

Employees of the Council are often provided with facilities, including office equipment such as computers, telephones, photocopiers and fax machines; transport, to use in carrying out their official duties. Telephones, photocopiers, computers and faxes are available to staff for private use, with authorisation from the Chief Officer. (See 11.2 below for Rules on personal use of telephones and computers) Personal use of any other Council equipment or removal of any property from the workplace and/or Council premises, for any purpose, is not permitted.

Where equipment or property owned by the Council is no longer required, employees may acquire such for their own private use, only with the authorisation of their ~~Chief Officer~~line manager. Depending on the circumstances and the value of the items, employees may be required to make a financial contribution to the Council, in line with guidance from Internal Audit.

Employees who wish to access, as a member of the public, property, facilities, services or equipment, which is normally provided by the Council on a commercial basis, must not gain any advantage by reason of their position. Where there may reasonably be a perception of potential conflict, employees must advise their ~~Chief Officer~~line manager that they propose to use such Council property, facilities, equipment or services, and their ~~Chief Officer~~line manager will guide employees on the appropriate action to take.

11.2 **Use of Council Communication Systems**

~~Employees using Council communication systems should note that t~~The Council has the right to~~, and will,~~ access and monitor ~~its communication systems to ensure their proper and effective uses by employees. Such communication systems include the Council telephone, e-mail and Internet.~~all of the communication systems it provides to an employee to do their job.

The Council will monitor employee usage of its Communication systems (telephone, email and Internet access), to ensure their proper use by employees and will run reports detailing Internet usage levels of Council staff.

~~The Council has the right of access to employees E-mail and other related computer files if required for investigation of misuse or excessive personal use. If misuse or excessive personal use is detected, this could result in disciplinary action for misconduct, and in serious cases could lead to an employee's dismissal.~~

Communication systems may be accessed when the Council suspects that the employee has been misusing council systems or facilities, or, for the investigation of suspected fraud or other irregularity (see 'misuse' below).

Access to emails will be confined to the address/heading and the Council will avoid opening emails clearly marked as private or personal, unless there is evidence of

suspected misuse. A limited number of staff will undertake such monitoring, and those that do will be made aware of Data Protection and confidentiality requirements.

Very exceptionally and where service deliver reasons exist, senior officers in IT may approve access to emails when an employee is absent.

Access to facilities may be temporarily suspended whilst an investigation is on-going and may be permanently withdrawn where misuse is detected. Cases of 'misuse' may result in disciplinary action being taken. This may include dismissal.

Time scales for retaining specific documents and/or information can be found in the 'Document Retention Schedule' located on the Intranet.

11.2.1 **Telephones and Mobile Phones**

Generally, employees should ~~not~~ use the telephone or ~~any~~other mobile ~~phone~~devices provided by the Council for ~~personal~~ business use only.

~~However the Council recognises that it is sometimes necessary for employees to make or receive personal calls during working hours. Any personal calls, which are made or received, should be brief, and where possible made in the employee's work breaks. Employees should keep to a minimum time spent making personal calls on private mobile phones, during working hours.~~

However where authorised, personal use outside of working hours of specific devices e.g. Blackberry's can be undertaken provided that all costs are paid in line with repayment procedures.

The Council recognises that in exceptional circumstances it is necessary for employees to make or receive personal calls, SMS or email during working hours. In these circumstances any personal usage should be brief, and where possible made in the employee's work breaks.

~~Employees should only use a Council business use mobile phone when absolutely necessary. Itemised phone bills are requested from employees who are provided with a mobile phone for business use.~~

~~Employees should be aware that t~~Telephone usage is monitored by use of the Call Logging System, which also records numbers dialled. The Council is able to listen to telephone calls for the purposes of monitoring customer service, investigating potential misuse of the system etc, and ~~may~~will do so from time to time.

11.3~~2~~.2 ~~——~~**E-mail and the Internet**

E-mail and the Internet are available for communicating on Council business. The following provisions for use of E-mail and the Internet also apply to access provided for remote use (e.g. ~~from home,~~ hand held, portable devices etc) ~~.~~and to home working employees using their own IT equipment outside of Council premises during working time or whilst undertaking council duties.

Employees' attention is drawn to the fact that external e-mail is not secure and that this must be taken into account in choosing how personal and confidential

information is communicated.

Employees must ensure that they do not make inappropriate comments in any emails. Employees should be aware that contracts formed by e-mail or over the Internet might be legally binding. Any contractual agreement, offer or acceptance must only be made by an employee via e-mail or over the I ~~i~~nternet where either the employee has authority to do this or where specific line-management authorisation has been given.

Good practice guidelines for the use of ~~E~~e-mail and the Internet are available from your ~~Departmental~~ IT section.

11.3.1 Personal use

It is recognised that from time to time, e-mail and internet facilities may be used for personal reasons unrelated to council business. Such use should be brief, outside of working hours (except in a case of emergency) and must exclude activities listed under 'misuse'. Excessive personal use of e-mail or the I~~i~~nternet is unacceptable and appropriate disciplinary action will be taken

11.3.2 Social networking websites

The council does not allow employees access to social networking websites for personal use (i.e. non- job related use) at all during work time.

The Council allows access to some journals, blogs and social networking sites during work time for the purposes of undertaking job related duties only. Employees must act in the best interests of the Council and not disclose personal data or information about any individual including service users, young people and children. This includes images. Access may be withdrawn and disciplinary action taken if there is a breach of confidentiality or defamatory remarks are made about the Council, it's service users, employees or managers.

The Council respects an employee's private life. However, it must also ensure that confidentiality and it's reputation are protected. Employees using social networking websites in their private life;

- must refrain from identifying themselves as working for the Council, or disclose the name of Bristol City Council on it, or allow it to be identified by details, which has or may have the effect of bringing the Council into disrepute.
- must not identify other Council employees or service users without their consent
- must not make any defamatory remarks about the Council, it's service users, employees or managers or conduct themselves in a way that is detrimental to the Council
- disclose personal data or information about the Council,or it's service users, employees or managers that could breach the Data Protection Act 1998.(e.g photographs, images)

11.3.3 Personal Websites and Blogs

Employees who wish to set up personal webforums, weblogs or 'blogs' must do so outside of work, not use city council equipment and adhere to the points detailed in 11.3.2 above.

Any breach of 11.3.2 or 11.3.3 whether nor not committed within work time and/or premises, could lead to disciplinary action up to and including dismissal.

11.3.4 Trade Union Representatives

Accredited Trade Union representatives can use Council communication systems for the purposes of undertaking Trade Union duties. See Time off for Trade Union Duties and Activities guidance..

11.4 Misuse

~~E-mail or Internet~~The Council's communication facilities must not be used for any activity~~,~~ which is illegal, unacceptable or inappropriate to the good conduct of the Council's business. Examples include:

(i) Creating, s~~S~~ending or forwarding any message that could constitute bullying or harassment (e.g. on the grounds of race, sex, disability) or who's content or intent would reasonably be considered inappropriate or unacceptable.
(ii) Participating in forwarding chain letters/ pictures/graphics etc
(iii) Accessing pornography
(iv) On-line gambling
(v) Committing or implying commitment to any contractual arrangements
(vi) Posting confidential information about the Council, ~~and/or~~ other employees and clients
(vii) Any illegal activities
(viii) Accessing any ~~inappropriate material including any material whose presence on Council systems might be prejudicial to public confidence in the Council.~~ non work related or otherwise inappropriate or unacceptable material
~~(ix) Messages who's content or intent would reasonably be considered to be abusive, disrespectful, hurtful or undermining~~
(ix) Accessing or forwarding .exe files
(x~~i~~) Mass-mailing/mail shots ("spamming") for specific personal views, gain or other personal use
(xi) Unauthorised use of Council facilities or employee's personal IT equipment, for personal use during the employee's working time

This list is not exhaustive and is also applicable to employees whilst they are undertaking city council duties using personal IT equipment. Any employee who is unsure about whether something he/she proposes to do might breach this policy should seek advice from their manager.

Employees receiving ~~such~~ inappropriate communication or material must inform their Manager immediately.

Employees should familiarise themselves with the Council's Data Protection Guide (link).

~~Due to the potential risk to the Council of E-mail, the Council monitors E-mail usage. Therefore, employees should not assume that any E-mails sent are private or confidential. The Council also monitors Internet Usage, including the sites visited.~~

11.2.3 ~~General Computer Usage~~

~~Employees are only permitted access to parts of the computer system, which are necessary in order to carry out their normal activities, or authorised personal use.~~

~~The following examples constitute computer misuse:~~

~~(i) Fraud and theft~~
~~(ii) Introduction of viruses~~
~~(iii) Loading and/or using unauthorised software~~
~~(iv) Obtaining unauthorised access~~
~~(v) Using the system for non-work related activities, including games during work time (Use of the system outside work time is permitted, providing the employee has received authorisation from their manager)~~
~~(vi) Breach of the Council's IT Security policy~~

~~**This list is not exhaustive**~~

Appendix (5) B -Web Access for Staff

Risk Assessment for relaxation of Internet usage rules

Risk	Ranking (probability/impact	Mitigation	Evaluation of Mitigation/comment	Residual Risk
Excessive non-business and inappropriate use by staff	H/M	Code of Conduct sets out rules.	The Code of Conduct for employees states that email and Internet facilities may be used for personal reasons unrelated to council business and that use should be brief, **outside of working hours** and exclude activities listed under misuse.	H/M
		Induction/other training Recruitment training	The Code of Conduct is covered by Corporate induction training which is mandatory for all employees who work in excess of 10 hours per week. The Code of Conduct is drawn to the attention of delegates at Recruitment & Selection training	
		Awareness campaign and periodic reminders		
		Continuing to block illegal sites and other sites with no business purpose	ICT maintain, update and implement a list of blocked sites.	
		Monitoring of top 20 highest Internet users	There are limitations as to what the monitoring information can provide. The	

			monitoring is only likely to identify the most extreme cases of misuse and relies on the manager having a good grasp of what their staff should be doing. If managers have concerns they will be advised to contact STS HR.	
		Performance management	Managers need the supportive tools. Existing resources could not cope with a significant increase in requests for Internet use reports on staff	
		Disciplinary and Performance Management policies	Processes here are lengthy and resource intensive. Cases likely to increase.	
Information Security Risk - using collaborative software tools with inadequate security for creating, storing, transferring BCC data	M/M	Block use of collaborative software as new web software being procured will be able to provide in near future.	Staff education and awareness Data classification	L/M
Misrepresentation of BCC in chat rooms, blogs etc	M/M	Code of Conduct Awareness campaign and periodic reminders	Enhancement to Code of Conduct in relation to social networking, personal web sites and personal web blogs	M/M
Increased risk of Malware eg viruses etc	M/M	Code of Conduct Information Security Policy Up to date firewall protection etc		L/M