

Public Document Pack



Stephen McGrath – Member Services Manager
General Enquiries: Telephone No. 01362 656870
Member Services Fax No. 01362 690821
DX743950 Dereham 2

To The Chairman and Members of the General
Purposes Committee

All other Members of the Council – for information

Your Ref:

Our Ref: DD/L.3.8

Contact: Diana Dring

Direct Dial: 01362 656354

E-mail: Diana.dring@breckland.gov.uk

Date 20 July 2010

Dear Sir/Madam

GENERAL PURPOSES COMMITTEE - WEDNESDAY 21 JULY 2010

I refer to the agenda for the above-mentioned meeting and enclose the following item.

6. Local Joint Consultative Committee: 8 July 2010

To adopt the unconfirmed Minutes of the Local Joint Consultative
Committee meeting held on 8 July 2010.

19 - 25

Yours faithfully

Diana Dring

Committee Officer

At a Meeting of the

LOCAL JOINT CONSULTATIVE COMMITTEE

**Held on Thursday, 8 July 2010 at 10.00 am in
Anglia Room, The Conference Suite, Elizabeth House, Dereham**

PRESENT

Employers' Side

Mr R.G. Kybird
Mrs S.M. Matthews
Mr K. Martin
Mr D.R. Williams JP (Chairman)

Staff Side

Mrs L. Heywood
Dr Z. Waterford (Vice-Chairman)
Mrs. R. Farman

In Attendance

Sheila Cresswell - Committee Officer
Natalie King - Principal Human Resources Adviser
Kevin J Taylor - Head of ICT

Action By

20/09 MINUTES (AGENDA ITEM 1)

As there had been some confusion about the actual meeting venue, the Chairman began the meeting with a formal request that all future meetings of the Local Joint Consultative Committee should be held in the Norfolk Room.

It was noted that Agenda Item 5 (Staff Forum) had been withdrawn and would instead be taken to the next scheduled meeting.

Zandra Waterford formally accepted the appointment as Vice-Chairman of this Committee.

Subject to these points, the Minutes of the meeting held on 1 June 2010 were confirmed as a correct record and signed by the Chairman.

21/09 APOLOGIES (AGENDA ITEM 2)

Apologies for absence were received from Mark Broughton.

22/09 DECLARATION OF INTEREST (AGENDA ITEM 3)

None.

23/09 ICT SECURITY POLICY (AGENDA ITEM 4)

Kevin J. Taylor, Head of ICT, presented this report which sought approval to issue the proposed new ICT Security Policy (2010). Once formally adopted, the revised ICT Security Policy (ICT SP) would be re-issued, enabling a formal sign-off of the document by all staff and Members.

As background, the Head of ICT explained that the current ICT SP had been formally agreed back in 2003 and although a new policy had been drafted in 2008, it had not been formally ratified at CMT or by the LJCC.

Action By

It was acknowledged – not least as a result of comments from both the internal and external auditors – that the Council needed to revisit this policy to ensure that it was current and had been formally adopted.

Other key driving forces for this included:

- growth and development in mobile technology and social media usage;
- the need for tighter security control and awareness for off-site working; and
- the need to clarify and formalise new user awareness of the Council's IT policy, as well as for all current staff and Members to be officially reminded of the existence and scope of this policy.

The Head of ICT then went through the proposed policy paper with Members, including input which he had received from the absent Mark Broughton where appropriate in the general discussion.

2 : Scope

2.1 : Who it applies to

It was confirmed that the policy would apply to ARP, as well as Breckland, staff.

2.3 : What it applies to

He also confirmed that the reference to social media applications was an addition to the previous ICT SP.

3 : Roles and Responsibilities

3.1.4 : Steria

He confirmed that whilst the ultimate responsibility for IT services remained with Breckland's ICT team, the wording in this clause would be broadened so that in the event that Steria were no longer the chief contractor providing IT services for the Council, this would cover whoever held this licence.

5 : Monitoring and Enforcement

5.1.3 : Dealing with Breaches

There was some discussion about this area, since it was acknowledged that there could be inadvertent access to inappropriate websites. It would therefore be important to ensure that the full picture was taken into account before any enforcement action was taken, or processes started.

Action By

The Head of ICT pointed out that any minor infringements would be logged but, unless they occurred on a regular basis – thus indicating possible abuse - these were unlikely to be followed up. The rules and regulations around internet usage and browsing should be clear enough to enable responsible usage, and the organisation should be able to trust its staff to adhere to this.

In response to a question, he confirmed that the IT team were able to see how long someone had been on a site. However, he added that care needed to be taken on this, since it was perfectly possible for someone to leave a site open but then move away from their desk, (i.e. not necessarily be actively engaged with the site for the whole time apparently indicated).

He also said that the IT team would not expect to undertake regular detailed monitoring, unless notified of possible misuse by line managers or others - not least because they lacked the manpower to devote too much time to this area.

In relation to informal warnings and “appropriate enforcement action” after minor or inadvertent breaches, it was therefore agreed to amend the wording in such cases to include an element of discussion with HR.

6 : Security Policies

6.7.3 : Use of Passwords

A Member raised concern about the statement that “passwords should not be written down”. For some people, working with different software packages - particularly those requiring frequent, brand new, passwords – this rule could be extremely difficult and impractical.

The importance of security around passwords was acknowledged, but the Committee agreed that there could be acceptable ways around this problem, such as having a specific location within each team where passwords could be recorded, with access strictly and appropriately monitored.

The proposal for passwords to be changed “at least every two months” was also discussed, since it was acknowledged that to some extent this could depend on the nature of the system in use, and/or the frequency of usage. However, the Head of ICT pointed out that as this was something which was set by Central Government, the Council would be unable to change this rule.

Action By

6.8 : Internet Usage and 6.8.1 : Using Email

The second paragraph, highlighting the fact that access to the internet for personal use should be 'on a limited basis, in personal time (i.e. generally during a lunch break), and only with the approval of the Service Manager', etc., caused some concern in terms of how practical and realistic this was.

In response, the Head of ICT said that this had been directly lifted from the 2004 version. He acknowledged that this could perhaps be refined. The word "reasonable", for instance, might need further clarification in this context.

Other points raised in general discussion around this policy included:

- There was no mention of the fact that some internet usage (perhaps even considerable amounts) might legitimately be needed for certain Council work.
- The need, therefore, was to monitor and define acceptable levels of personal usage. This should be given further consideration, not least in relation to current employment law.

It was agreed that any Member or Council employee effectively running a business (for commercial gain) whilst using Council equipment and on Council time, would certainly be abusing the policy.

However, it was acknowledged that in modern society an element of personal usage was generally considered acceptable during working hours or lunch breaks (e.g. medical/childcare/carer/school arrangements, booking holidays and some limited personal banking, etc).

Another point raised was the fact that the staff intranet offered a facility for staff sales. However staff might also be permitted to use auction sites in their own time, subject to line managers' discretion.

The Group felt that provided general permission had been sought, and that this was done during the lunch break (and not to excess), this sort of personal usage should not be considered unreasonable.

On balance, the Security Policy should be robust, but not overly prescriptive, and it should allow a level of flexibility. One way around this could be for the policy to make clear distinctions between what it defined as 'commercial' and 'private' usage. It was felt that there might be a need for further discussion in this area.

Action By

- It was also pointed out that the final sentence on page 16 was unfinished and should read: "N.B. Internet usage stats are recorded and issued on a Monthly basis."

However, during further discussion on this, the Head of ICT confirmed that whilst they could produce such statistics for individual accounts, this was hugely resource-intensive and not generally done as a matter of course.

- There was also some comment about the final paragraph of 6.8, and whether or not the word "sensitive" could be further clarified, perhaps by giving some examples, to confirm exactly where lines were drawn within the legal framework.

6.9 : Working at Home or at a Remote Location

The Head of ICT explained that although in the office there were robust Health and Safety measures, there was also a requirement to visit relevant homes to undertake appropriate risk assessments. However, he added that there was a clear distinction between those who worked at home (i.e. on an ad hoc basis), and 'home workers' (as defined in the ARP Home Worker policy). The proposed Security Policy purely referred to those occasionally working at home.

The PAT (electrical) tests were undertaken on Council-owned lap tops, which were the recommended tool when working from home (as opposed to using personal IT equipment - not least since such equipment would not comply with the various levels of security software).

It was felt that Members and staff should be reminded about the need to take great care in terms of the content of any emails sent as part of Council business when working off-site. The Head of ICT added that his team intended to have a tighter control on the use of Memory Sticks, and this was currently under review. It was also noted that there was always an option to seek a loaned laptop for occasional home use.

In conclusion, the Committee therefore **Agreed:**

- (1) **3.1.4 : Steria:** The wording in this clause would be broadened to ensure that this covered whoever was responsible and held the licence.
- (2) **5.1.3 : Dealing with Breaches:** With reference to minor or inadvertent breaches, the wording should be amended along the lines : "... will be discussed with Human Resources and necessary action taken."

Action By

- (3) 6 : Security Policies: To delegate authority to the Head of ICT and the HR team, in terms of Employment Law, to produce a more appropriate form of wording for this section of the Policy. This should include examples of acceptable forms and lengths of personal usage of the internet.
- (4) With respect to passwords, the wording should be changed along the lines:

“Ideally, passwords should not be written down, but if they are recorded they must be stored securely and appropriately.”.
- (5) The “*overall* approval” of Service Managers for internet usage should be sought, rather than “approval”, as currently cited, since the latter implied approval being needed on every occasion.
- (6) To delete the sentence concerning Internet usage statistics being recorded and issued on a monthly basis.
- (7) To consider whether or not the word “sensitive” at the end of Section 6.8 could be clarified further by the use of examples, in order to confirm exactly where lines were drawn within the legal framework.
- (8) Steria’s full telephone number to be inserted in the first paragraph of Section 6.8.1 (Using Email).
- (9) In terms of Working at home or at a remote location, the ICT team would have a tighter control on the use of Memory Sticks. They might also have a spare lap top available for wider use. In addition, the Member Support Officer would be required to add a visual examination to his current check-list in terms of IT equipment used at home by Members.
- (10) To change the title at 6.10 to read “Mobile Phones/Blackberry and Portable Devices”.

24/09 STAFF FORUM (AGENDA ITEM 5)

As mentioned earlier, this item had been withdrawn and would now be considered at the next meeting. This was because the staff side wanted to resolve a few further issues before they felt it appropriate to discuss this matter at the Local Joint Consultative Committee.

The Chairman reminded Committee Members that it was important to ensure that the Committee Services Team were kept fully informed at all stages, in order to avoid inaccuracies on published agendas.

Action By

25/09 NEXT MEETING (AGENDA ITEM 7)

It was noted that the next meeting would be held on 16 September 2010.

The meeting closed at 10.55 am

CHAIRMAN

VICE-CHAIRMAN