

**Systems Review Action Plan: Security of Data S.024.10****Action Plan 1****Date Issued : Oct '10**

| <b>Ref. No.</b> | <b>Finding</b>  | <b>Recommendation</b>  | <b>Priority</b> | <b>Management Comment</b>   | <b>Manager Responsible</b>                                 | <b>Date of Action</b>   |
|-----------------|---|--|-----------------|---|--|---|
| <b>1a</b>       | <p><b><u>Improvement Grants - Security</u></b></p> <p>Files containing personal details were held in an unsecured store room outwith the area restricted to staff through secure entry doors.</p> | <p>It is recommended that, in consultation with other users, arrangements are made for the store room to be locked to prevent unauthorised access.</p>   | High Risk       | <p>Store room door secured and locked – access now only available to staff with key obtainable from Front office staff. Door returned to secured state on completion of file retrieval.</p>   | <p>Colin Newman<br/>Team Leader<br/>Building Standards</p> | <p>06/10/10</p>   |
| <b>1b</b>       | <p><b><u>Improvement Grants - Document Retention</u></b></p> <p>Files are not held in accordance with the document retention policy prescribed periods.</p>                                       | <p>It is recommended that, in order to comply with data protection requirements and the Council's document retention policy, there should be an annual review of stored material as a check to ensure that there are no documents being retained beyond their agreed retention period, i.e. an annual purge should be carried out.</p> | Low Risk        | <p>Review now being undertaken to identify files that may now be disposed of in accordance with Council document retention policy. Once identified, relevant files will be destroyed by shredding and record kept of the destruction authorisation – this will be done in accordance with retention policy.</p> | <p>Colin Newman<br/>Team Leader<br/>Building Standards</p> | <p>Review started<br/>06/10/10<br/>Due to anticipated volume<br/>Target completion<br/>20/12/10</p> |

**Systems Review Action Plan: Security of Data S.024.10****Action Plan 1****Date Issued : Oct '10**

| <b>Ref. No.</b> | <b>Finding</b>  | <b>Recommendation</b>   | <b>Priority</b> | <b>Management Comment</b>  | <b>Manager Responsible</b>                     | <b>Date of Action</b> |
|-----------------|---|---|-----------------|--|--|-----------------------|
| <b>2</b>        | <b><u>Treasury Management - Document Retention</u></b><br>Files are not held in accordance with the document retention policy prescribed periods. | It is recommended that, in order to comply with data protection requirements and the Council's document retention policy, there should be an annual review of stored material as a check to ensure that there are no documents being retained beyond their agreed retention period, i.e. an annual purge should be carried out. | Low Risk        | Within the Treasury Management Code of Practice there may be requirements to keep documents for longer periods than the Council's document retention policy – however a review of all files will be undertaken prior to the end of the financial year and compared with both the Council policy and the TM Code of Practice. | Jennifer Ogilvie<br>Section Head<br>(Treasury) | 31/03/11              |

**Systems Review Action Plan: Treasury Management****Action Plan 2****Date Issued: Oct 2010**

| <b>Ref. No.</b> | <b>Finding</b>  | <b>Recommendation</b>  | <b>Priority</b> | <b>Management Comment</b>  | <b>Manager Responsible</b>                 | <b>Date of Action</b> |
|-----------------|---|--|-----------------|--|--|-----------------------|
| 1.              | Certification of Reconciliations<br>Some of the Treasury Reconciliations as at 31st March 2010 had not been certified by a senior member of staff.  | It is essential that senior staff certify all reconciliations to confirm that they balance and are being kept up-to-date.  | Medium Risk     | Reconciliations are now being certified as checked.  | Gillian McNeilly,<br>Manager of Accounting | Already actioned      |
| 2.              | Risk Management<br>Although the Treasury Management Practices include a detailed statement on risk management, they have not been incorporated into either the Corporate Services/Finance or the Council risk register. | It is recommended that the Treasury Management risks are included in the Corporate Services risk register in order that senior management can continue to monitor and control the adequacy of the management of these risks. | Low Risk        | These will be incorporated into the Finance risk register.   | Gillian McNeilly,<br>Manager of Accounting | 31st December 2010    |
| 3.              | CHAPS Access<br>A member of staff, who has been on maternity leave for nine months is still an authorised user of the CHAPS automated payment system.   | Where it is anticipated that staff will be off for a considerable period, it is recommended that their access to the CHAPS system be withdrawn.  | Medium Risk     | Action will be taken to ensure that anyone no longer dealing with CHAPS payments for a period of time will be removed from the authorisation list. | Gillian McNeilly,<br>Manager of Accounting | Already actioned      |