KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

P1 & P2 AUDIT RECOMMENDATIONS ONLY

IT NETWORK CONTROLS 2006/07 [Follow up May 07]

P2 That a formal timetable is drawn up for the creation of a formal Information Strategy.

P2 That the Business Development Manager ensures that there is a timetable in place to regularly review and update the Security Policy and the Computer Strategy, once it has been produced.

P2 That formal training sessions should be given on the Security Policy.

P2 That the Business Development Manager reviews the structure to ensure that it reflects the true position and the job descriptions to ensure that they clearly define the roles, duties and responsibilities and that Information security is formally defined within the job descriptions.

P2 That Human Resources ensure that all employees receive a job description which defines their roles, duties and responsibilities prior to them commencing their employment. A copy of this job description should be signed by the employee and kept on the Human Resources file.

P2 That the ICT Team Leader ensures that there is a timetable in place for the compilation of the office manual.

P2 That the ICT Team Leader ensures that there is a plan of proactive work which covers at least the next 12 months.

P2 That the ICT Team Leader (System Support) has the Service Level Agreement formally adopted and agreed with the other departments and 3rd parties.

P2 That the system is amended to enforce password security of being a minimum length of 6 characters and be a mixture of symbols, numbers and letters.

P2 That there should be documentation to support the ongoing use of the super-user accounts on the Unix box which are used for support of the FMS and Academy systems. These should be authorised by a senior manager.

P2 That IT ensure that they do not set up a new user until they are fully aware of the type of contract that they are employed on.

P2 That, whenever a contract, temporary or fixed term employee is set up by IT, that an expiry date equal to the last date of their expected contract is set on their password.

P2 That the Human Resources Department is made aware of all contract staff employed by the various departments and their expected end dates. [e.g. there may be a need to sign a confidentiality agreement]

P2 That Human Resources send a copy of the starters' form (which should include movers to new posts) to the IT section, in advance of the start date.

KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

P2 That users should only be set up when their access rights are authorised by their line manager. There should be documentary evidence of this e.g. helpdesk form.

P2 That managers review user access at least annually e.g. as part of employee development interviews.

P2 That managers retain a record of who attends training courses. [We note that the new Performance Management Software, to be rolled out towards the end of 2006, will incorporate the facility to record training attended. This will need to be maintained by managers.]

P2 That a record is maintained of all back-ups. This should show details of all tapes stored and where and this should be checked periodically for accuracy and signed off by a senior IT support member as correct.

P1 That the level of insurance cover for the replacement of software is reviewed and amended to an adequate level.

P1 That a formal timetable is drawn up for the completion and approval of a formal Disaster Recovery Plan of the Council. This is to include the network is respect of servers, communication links, personnel and critical stationery. It should also include the requirements of users, clients etc. in terms of what is required of them in respect of their duties, stationery etc. The plan then needs to be tested.

The following recommendations were made by the external computer auditor:

P1 That the Council should provide the resources for the implementation of an IT technical training programme, part of which should involve the sharing of the expertise currently resting with the IT Technical Team Leader.

P2 That the IT Technical Team Leader, should undertake a full risk assessment of the Council's network, resulting in the production of a Network Access and Control Document.

P2 That, in order that the network diagrams are relevant and up-to-date, each diagram should be given a meaningful title and marked with issue date and author. An up-to-date document/diagram of the Server/Communications Room should be produced. The network physical diagram should be updated to include the Academy server.

P2 That the process of updating the network logical diagrams should be completed as soon as possible.

P2 That, in order to clarify the individual and joint responsibilities for the management of and changes to the network, and ensure that both planning and day-to-day practice serves the needs of the Council, a local agreement should be established between IT and Kier management. Copies of the Bailey's review of the network should be retained by the IT Department.

P2 That an Information Incident Reporting Policy should be established and appropriate procedures written to cover network and other security incidents.

KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

P2 That the results of penetration tests, performed by external consultants, should be retained as evidence of effective firewalls and security software, and to identify any weaknesses, and required corrective action.

P2 That the IT Technical Team Leader should consider acquiring and using software to highlight intrusion attempts.

P2 That the IT Technical Team Leader should document Standards and procedures for preventing and detecting intrusion.

P2 That Procure Manager software should be reviewed to find out why it does not provide full details of work undertaken on network devices. If the software is unable to maintain details of network changes made, then a manual log should be maintained.

P2 That the Authority should ensure that it holds an up-to-date copy of the warranty agreement with HP, for maintenance of servers, and maintain a log of associated work undertaken.

P2 That a record should be maintained of changes to the network, operating system upgrades, replacement of servers, etc to include:

- the date of the change
- who carried it out
- the release and/or patch reference.

P2 That entry to the Server/Communications Room should be controlled by card.

P1 That written confirmation should be obtained to ensure that there is no potential health and safety issue relating to the release of the Argonite gas into occupied rooms.

P1 That there should be a local 'Duty of Care' arrangement in place for IT staff working alone in the Server/Communications Room or at remote sites.

P2 That the IT Department should ensure that cabling in the switch/communications room 17 should be "neatly bundled".

P2 That the document 'Secure Portal Access' should be extended to cover all remote users, and include the method of access, authorisation requirements and type of access that will be provided.

P2 That the ICT Team Leader should document a user registration procedure for remote users, covering access administration responsibility, authorisation, registration, de-registration, review of access, etc.

P2 That a current list of authorised remote users should be retained, identifying the type of access each user has been given.

P2 That assurances should be obtained from the users that remote access is controlled by the Revenues and Benefits access administrator, and that Academy only have access to the system on a 'needs to access' basis.

KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

FREEDOM OF INFORMATION ACT 2006/07 [Follow up April 2007]

P2 That, as a minimum, a section on Freedom Of Information (FOI) is included on the Induction Form which should be completed by managers when a new starter is appointed.

P2 That employee awareness is raised regarding FOI.

P1 That outstanding work re records management should be identified and resources identified to implement the requirements. This should include a review of document structure to facilitate compliance with the publication of information. The timing of any audit review of this area is to be agreed with management.

P1 That the Publication Scheme is updated to specify the manner in which information of each class is, or is intended to be, published.

CASH RECEIPTING 2006/07 [Follow up April 2007]

P1 That the Customer Services Team Leader (Cashiers) should set the user access parameters to enforce a change of password every 40 days, in line with the corporate Security Policy.

P2 That Academy templates are revised to show that Council Tax and NNDR payments can be made on the website and that the website address is updated to **www.copeland.gov.uk**.

P2 That signs should be clearly displayed in the cash offices stating that:

- an official receipt must be obtained for any cash payments made
- cheques must be payable to Copeland Borough Council

P2 That validation codes should be added to the cash receipting system for the following funds:-

- Planning
- Waste Management
- Building Control
- Land Charges
- Licensing
- Car Parks

These funds have a limited number of FMS codes to set up for the validation routine and this would eliminate many of the input errors.

P2 That, until the above can be implemented, the Customer Services Team Leader should review the Full Transaction Listing report on screen for each cashier, as part of the cashing up routine. This would clearly show if e.g. the FIRSTBREG code (Building Control) had been entered as FIRSTBREGS or had been entered against Fund 1 (Planning) instead of Fund 7 (Building Control). Where funds have numerical FMS codes consisting of 9 digits, a review on screen would also immediately show where a digit had been added or omitted, as the transaction would be out of alignment with the

KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

other correct transactions. The errors could then be corrected by the cashiers before the cash receipting system is updated to the FMS.

P2 That all suspense items should be promptly cleared but, if this is not possible given staff resources, then those items over £50 should be prioritised for action.
[Relates to Benefit Overpayments Unallocated items]

P2 That a receipt made out in error must have "Cancelled" written on it and the cancelled receipt must be stapled to the collection sheet, as evidence that no payment has been made for this transaction.
[Relates to manual receipts]

P2 That all area offices keep a record showing the sequential numbers of cash collection sheets issued to them and the date each sheet was used.

P2 That, where unidentified items cannot be input by the cashier, the cashier should record the date and her initials against the item on the listing to show that this item has been excluded from the processing.

P2 As at 11/10/06, written procedures for post opening were being updated. Progress to be checked as part of the audit follow up.

P2 That the Customer Services Team Leader (Cashiers) check whether the reason for reversal field was, in fact, mandatory or whether it could be ignored.

P2 That the Customer Services Team Leader (Cashiers) investigate the missing items from the Reversal Listing report and to check the reason for this with the Helpdesk if necessary.

P2 That a cumulative record is kept of overs/shorts, listed by cashier, and that the Customer Services Team Leader uses this to monitor for error rates / irregularities.

P2 To improve the accuracy of the automatically generated overs/shorts reports, we recommended that cashiers double check the input of totals for cash/cheques etc. before the cashing up procedure is completed. At this point, errors can still be corrected.

P2 That the cashiers' takings at the Copeland Centre cash office are checked by a second person, at the point of handover at the end of the shift, before they are placed in the safe overnight.

P1 That same day banking for cheques of £10,000 or more be resumed with immediate effect (27/10/06).

P2 That, where there is no reference or account number, identifying details must be entered in the narrative in the cash receipting system.

P2 That the cash posting routine to NNDR Pro IV is always run on a daily basis.

P1 That progress on fitting the 3rd panic alarm and the value of cash held on the premises should continue to be monitored.

KEY RECOMMENDATIONS FROM REPORTS ISSUED
[Bold text in brackets shows the management response]

P1 That verbal instructions should be given to all cashiers on the appropriate action to take in the event of a raid. Written procedures should then be updated to include this issue.

P2 That Corporate Team agree the priorities / timescales for the reinstatement of all Council IT systems. This will form the basis of individual service-level business continuity plans. Service Managers will then need to consider what measures could be put in place pending reinstatement of their IT systems.