

Authorisation protocol for investigating allegations of breaches of the Internet and Email Acceptable Use Policy

Monitoring is a recognised component of the employment relationship but employers must take care to ensure that any monitoring policy does not amount to a breach of the Data Protection Act 1998 or the Human Rights Act 1998 and that it complies with the Employment Practices Code issued by the Information Commissioner's Office. The least intrusive form of monitoring should be used to fulfil a clearly stated business objective. For example; managers and colleagues looking through another employee's inbox in their absence in order to respond to urgent emails should not open emails that are clearly personal. Unopened emails that are clearly personal should only be opened in exceptional circumstances and should not be opened without first seeking legal advice.

When undertaking any form of monitoring or investigation, it is always necessary to balance the rights, freedoms and legitimate interests of the employee against the legitimate interests of the Council. Following this protocol will assist the Council in avoiding breaches of the Human Rights Act 1998 and the Data Protection Act 1998.

Accessing an employee's emails stored in personal folders or a history of Internet activity

This protocol outlines the procedure to be followed when an employee is suspected of having breached the Internet and Email Acceptable Use Policy and where a manager is of the view that further investigation is required. The Employment Practices Code is clear that personal information about workers should not be accessed if the intrusion into workers' privacy would be out of proportion to the seriousness of the matter under investigation. The steps below should be followed in each case before the Transformation Service is contacted to 'unlock' the required information.

Protocol

Concerns about potential breaches should be escalated to senior management level or above and the senior manager should take the following steps should they consider that it is necessary to access stored emails or to obtain detailed information about an employees Internet use;

1. The form Application for Email and Internet Data Form should be completed.
2. The form should then be forwarded to Audit Services who will assess the request as detailed on the form and consult with the requesting Department as necessary to determine whether the request is necessary, proportionate and appropriate. A record of the request will

be maintained in the central database of Internet and Email requests. The form will then be passed to Legal Services for consideration along with any other evidence to support the request.

3. After consideration by Legal Services the form will be returned to Audit Services, who will record the application and forward a request to the Transformation Service for provision of the approved information direct to the Departmental Manager initiating the request.
4. Consideration of the form will be prioritised by both Audit Services and Legal Services upon receipt.
5. Transformation Service should not provide access to personal folders or a history of Internet activity without having been provided with a completed form which has been signed by both Audit and Legal Services.