

Report to: Children Young People and Families Scrutiny Committee

Date: 17 September 2009

Subject: Response to theft of laptop in January 2009

Report of: The Executive Director of Children and Young People's Services and the Executive Director of Business Support Services

Contact officer: Tim Turner 01942 488354

Purpose / summary: To provide members with a summary of actions taken as a result of the theft of a laptop containing personal data from Progress House in January 2009.

Alternative options considered and reason for selecting the one recommended: None

Recommendation / decision: For members to note the contents of the report.

The decision will be made as a result of this report and will be published within 48 hours

Risks / Implications:

Financial:
Staffing:
Policy:
Equal Opportunities - Has a Diversity Impact Assessment been conducted?
Wards affected:

Property Implications – Does the proposal involve a reduction, addition or change to the Council's asset base or its occupation?

No

If yes, have the property implications been agreed with the Corporate Property Officer?

Does this proposal have significant implications for the Council and the local population?

A diversity impact assessment is not necessary at this stage, however, equality and diversity implications have been considered when producing this report.

Does this proposal involve a new policy or procedure or significant changes to an existing policy or procedure?

A diversity impact assessment is not necessary at this stage, however, equality and diversity implications have been considered when producing this report.

Has the Service Director - Borough Solicitor confirmed that the recommendations within this report are lawful and comply with the Council's Constitution? **No ***

Has the Service Director - Corporate Services confirmed that any expenditure referred to within this report is consistent with the Council's budget? **No ***

Are any of the recommendations within this report contrary to the Policy Framework of the Council? **No ***

* delete which applicable

For Cabinet reports only :

Categorisation of the report:	x		
Discussion leading to a decision		Discussion	
Monitoring		Decision	
Sharing for corporate understanding		Information	x

Tracking/Process:

	Consultation	Ward Members	Partners
CYPF Scrutiny Committee	Overview & Scrutiny	Cabinet	Council
17.09/09			

There are no Background Papers to this Report within the meaning of Section 100D of the Local Government Act 1972.

Proper Officer



Date

19th August 2009

Theft of a laptop containing personal data from Progress House

1. Incident involving loss of records
 - 1.1 During a burglary, a number of laptops were stolen from Progress House on 29 January 2009. One of the laptops contained a copy of the Fischer Family Trust database. This version contained information on most children and young people in Wigan schools: names, dates of birth, postcodes, ethnicity and, if applicable, special educational needs status and eligibility for free school meals.
 - 1.2 The Council's data protection policy states that:

“Electronic data must only ever stored in official server rooms. If this is impractical, data must be only stored in locations agreed by the Data Protection Officer in consultation with the Computer Section.

It is Council policy to store data on a network server where it is regularly backed up.

All valuable files and documents must be stored on the appropriate server on the Council's network and not on Desktop PCs or laptops.”
 - 1.3 The storage of data on the laptop was a breach of this policy. The Information Commissioner, who regulates Data Protection, states that personal data should only be stored on a laptop which is encrypted. Encryption scrambles the data on a machine and makes it all but impossible to retrieve without the password. The Commissioner's guidance states that any loss or theft of data, or of equipment containing data about more than 1000 people should be reported to his office, and we reported the matter to his office in February.

2. Action taken against the Council as a result

The Information Commissioner's staff investigated our report, and decided in July that the Chief Executive should be asked to sign an undertaking on behalf of the Council. The undertaking requires the Council to encrypt all laptops which contain personal data which could cause damage or distress if lost or stolen. It also requires the Council to train staff in the requirements of Data Protection, to ensure that staff are aware of Council policies on data, and to take any other steps necessary to ensure that the Council complies with the relevant Data Protection principles.

3. Laptop Audits & Laptop Policy

- 3.1 The Council carried out a laptop audit in February and March, identifying all laptops, laptop users and what laptops were being used for. This has been kept up to date since, as new teams receive machines, and as other laptop users are identified. The purpose of the list from now on will primarily be to track which machines have been encrypted, and to ensure that individual machines or teams which need encryption can be identified.
- 3.2 A detailed list of instructions for the safe and appropriate use of laptops was sent to all laptop users via the LAN Consent system once the audit was concluded in March.

Anyone subsequently added to the list of laptop users will automatically receive this list of instructions once they log into their computer.

- 3.3 Messages about the safe use of laptops were also cascaded to all managers, and communicated to staff via the Council's intranet and in the One Wigan staff magazine.

4 Encryption

- 4.1 Laptops issued to social workers in both CYPS and Adult Services were encrypted before they were issued. Machines which could in theory be used to store the most sensitive data about people were protected from the beginning. All new laptops have been encrypted as standard since January, and any brought in for routine repair or update are also encrypted. An initial group of CYPS teams were identified and their laptops were encrypted in May and June.

- 4.2 Following discussion with managers, a larger group of teams in CYPS were identified as being appropriate candidates for encryption. Although the number of officers who anticipated that they might need to store data on their machines was very small, but managers felt that it would be safer to encrypt their teams' laptops as a precaution. On this basis, a second wider programme of encryption will start from the end of August, running into November. Although the Commissioner's undertaking mentions the loss of data which might cause damage or distress, the programme is being done on a team basis to capture as many laptops as possible.

- 4.3 Once this second programme is up and running, any teams in Adult Services or other parts of the Council who could possibly store personal data on their laptops will be identified and included. The programme may therefore be extended beyond November if the need arises.

5. Training

- 5.1 The Data Protection Officer is organising a programme of Data Protection training for staff in all departments, in conjunction with the Learning and Development team. More than 200 staff were trained at the end of July as a trial, and further sessions will be held from September throughout the rest of 2009, with a view to training as large a number of staff as possible. This training will become mandatory for staff who routinely handle sensitive personal data.

- 5.2 Another Council which suffered a similar loss of data is using an e-Learning package to train staff – the Data Protection Officer will be informed of the success of this exercise. If it is judged to be successful, proposals will be drawn up for a similar approach in Wigan. For the time being, the training will be delivered face-to-face by the DP Officer.

6. Data Protection Audit

- 6.1 The Data Protection Officer has interviewed staff in Business Support Services and Children and Young Peoples Services as part of an audit of the Council's Data Protection practice. This process has been largely positive, but as a result, further advice on office security and data handling will be provided to all departments to supplement existing guidance available on the Council intranet. This process will shortly follow in Adult Services and other parts of the Council.

7. Future actions

- 7.1 Once the formal process of dealing with the requirements of the Information Commissioner is complete, and the second wave of encryption is in operation, other issues will be addressed. The Council will be conducting spot checks of laptops and other mobile devices to ensure that they are being used in accordance with Council policy.
- 7.2 A review of acceptable use and information security policies was already in progress, and lessons from the loss of the laptop will inform this process.

