DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Shropshire Council

Shirehall
Abbey Foregate
Shrewsbury
Shropshire
SY2 6ND

I, Kim Ryley, Chief Executive of Shropshire Council (the Council), Shirehall, Abbey Foregate, Shrewsbury, Shropshire, SY2 6ND, for and on behalf of the Council hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Shropshire Council is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by the Council and is referred to in this Undertaking as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the "Commissioner") was provided with a report from the Council regarding a memory stick containing a social care management database. The memory stick was lost during postal transfer from Shropshire Council's offices to a regular contractor based in Cardiff.

3. Sensitive data was transferred onto a password protected but unencrypted memory stick in breach of Council procedure. The information related to 3554 social care clients and 188 members of staff. The memory stick was sent in inadequately protected packaging, and contained records that were excessive for their purpose and out of date. The Council's investigations into the incident revealed a number of other shortcomings regarding localised data storage and transmission procedures, which have also been taken into consideration.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Third and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such

information is defined as "sensitive personal data" under section 2(e) of the Act.

5. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation ensure that personal data are processed in accordance with the Third and Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) Databases should only contain information relevant for their purpose and for the process of transfer;

(2) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted by no later than 30 April 2010 using encryption software which meets the current standard or equivalent;

(3) Personal data should only be transferred to removable media when absolutely necessary. Where possible, sensitive personal data should be accessed remotely or hand-delivered. All other post should be adequately tracked and protected;

(4) Adequate checks are carried out on contractors' staff to ensure that data processors are complying with the data controller's policy in respect of the storage and transfer of such data ;

(5) The policy covering the transfer, storage and use of personal data is reviewed to ensure compliance with the Act, particularly in respect of the security of the means of transfer and relevance of the data transferred;

(6) Staff are aware of the data controller's policy for the storage, use and transfer of personal data and are appropriately trained how to follow that policy;

(7) The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage.

Dated.....

Signed.....
Kim Ryley
Chief Executive
Shropshire Council

Signed.....
Mick Gorrill
Assistant Commissioner Regulatory Action Division
For and on behalf of the Information Commissioner

Mr Richard Kerr Enforcement Team Manager
Ms Daniela Guadagno, Enforcement Officer
Information Commissioner's Office
Wycliffe House, Water Lane
Wilmslow
Cheshire SK9 5AF

7 June 2010

LR

Dear Daniela and Richard

ICO MEETING - 26TH MAY 2010

I write to update you on the plans agreed following our meeting earlier this week when you met with fellow officers and myself to explore our activity following recent incidents and, to impart best practice to benefit further our management of sensitive information.

Following on from our meeting we have agreed a set of actions further to our present undertaking. These include–

- progressing the implementation of CRB e-bulk form processing services;
- Seeking positive confirmation from Directorate representatives that no personal data is being stored on unencrypted memory sticks;
- an audit of external data transfers and the current back up arrangements of the ALFIE system. As well as introducing a standard check on all audits, checking data security with specific focus on personal data;
- providing guidance through our officer Information Governance Group (IGG) on how service areas should engage with contractors and ensure security of data;
- securing 'wheelie bins' confidential shredding for HR services, in addition to our present confidential waste process;
- reviewing and updating guidance for staff taking personal data off site;
- circulating the Data Protection handbooks to high risk areas (payroll, personnel) and IGG representatives and
- following up with a free ICO Audit in the future

Our action plan also reflects the ICO's agreement to update the current Letter of Undertaking for memory stick/laptop encryption to September 2010.

I would like to take this opportunity on behalf of the Council to thank both of you for your time and support at the meeting and commitment to continuing support in the future.

Yours sincerely

Laura Rowley
Director of Resources

<casework@ico.gsi.gov.uk>
01/06/2010 11:44

To <Kim.ryley@shropshire.gov.uk>
cc <roy.morris@shropshire.gov.uk>, <Laura.rowley@shropshire.gov.uk>, <alvin.west@ico.gsi.gov.uk>
bcc
Subject ICO response[Ref. COM0303242]

History: This message has been forwarded.

Dear Mr Ryley, Mr Morris and Ms Rowley

Further to our meeting on 26 May 2010 and on receipt of Ms Rowley's letter dated 28 May 2010, this office is now in a position to provide a formal response regarding the security incident involving the loss of some 95 completed CRB forms.

At the outset, I would like to thank you for taking the time, along with your colleagues, to discuss the relevant data protection matters with myself and Richard Kerr at our recent meeting. I trust this was beneficial for the Council in terms of identifying areas for improvement or review, and in order to clarify any data protection concerns or queries the Council may have had.

With regard to the current file, some of the personal data contained on the CRB forms is of relatively high sensitivity and its disclosure could be detrimental to the individuals concerned, if compromised. It was also noted with some concern that the Council chose not to inform the affected data subjects that their information had been lost.

As you are aware, the Data Protection Act 1998 requires that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The Act states that 'Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—
(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and
(b) the nature of the data to be protected.'

The measures taken should be in proportion to the detriment that could be caused to the data subjects if their personal data were to be compromised. This will obviously depend on the nature of the information involved.

The remedial measures you have outlined appear proportionate to the detriment that may be caused to the data subjects, and to address the security issues in this case. It is noted that a council-wide risk assessment of personal data handling has been implemented, and that staff training and awareness of such matters has been significantly increased. This office was reassured to learn that the removable and portable media encryption programme is nearing completion

although it is acknowledged that some laptops are still outstanding. In recognition of the Council's efforts in this regard, the Information Commissioner will extend the encryption deadline (specified as 30 April 2010 in the Council's previous Undertaking to the Information Commissioner) to September 2010.

After meeting the CRB team and observing the manner in which their work is carried out, this office is confident that appropriate improvements have been made to the various procedures involved in terms of form processing and general personal data handling. During our visit, the disposal and destruction of paper documentation was also discussed, and the Information Commissioner welcomes the Council's suggested amendments to such procedures. As mentioned at our meeting, this office would also suggest that the CRB form retention periods are reconsidered and reduced where possible.

The fact that external data transfers now have to be approved at director level is an additional measure which will minimise the risk of further data losses as a result of insecure means of transmission, and it is assumed that this process will be continually monitored.

The security breach in question, along with the previous file under reference COM026193, involved the sending of personal data in the post, raising concerns that the methods of postage and packaging were insufficient. The Information Commissioner trusts that this has now been addressed across the Council to ensure that protection levels are proportionate to the nature of the data being transferred. This office would generally encourage secure electronic means of transfer wherever possible, and it is noted that a secure portal has now been set up in order for the Council to be able to receive data from third parties.

Although not strictly covered by the Act, as discussed during our visit, the Council may wish to consider placing an increased emphasis on the possibility of disciplinary action for any employee who contravenes policy. This may act as both a deterrent and serve to reinforce the assertion that the authority takes its data protection responsibilities seriously.

As you will be aware, new powers have recently been afforded to this office, which enable the ICO to impose monetary penalties for serious breaches of the Act. This further highlights the importance of all organisations ensuring their data protection procedures are suitably robust.

Ms Rowley's letter of 28 May confirms that several additional courses of action will be pursued by the Council following our meeting, in order to ensure data handling is secure across the organisation. The ICO welcomes these measures and strongly supports the Council's decision to implement them.

The possibility of an ICO audit has also been explored, with the view that it may be best to conduct this after the Council have had time to implement any proposed improvements, which is likely to be after September this year. It is felt that an audit will be highly beneficial to the Council in terms of data handling on an organisational level, and the ICO look forward to making the appropriate arrangements. Alvin West: Team Manager - Audit (which now forms part of the ICO's Good Practice Department), will be in touch shortly to discuss the matter further. You can contact him directly at: alvin.west@ico.gsi.gov.uk or on 01625

545 875.

After careful consideration of the facts of this case based on the information you have provided (and further to our meeting), it does not seem appropriate for the Information Commissioner to take formal regulatory action on this occasion. Although the Council provided an Undertaking to this office in December 2009 following the loss of an unencrypted memory stick, it has been borne in mind that the second incident occurred prior to the issuing of the Undertaking and before the Council had been able to fully implement the remedial measures specified.
However, both cases may be revisited if there is another incident of this nature involving Shropshire Council in the future.

Thank you for your assistance and cooperation in this matter.

Yours sincerely
Daniela Guadagno

Daniela Guadagno Enforcement Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. 01625 545647 F. 01625 545738 www.ico.gov.uk