Data Protection Act 1998

Monetary Penalty Notice

Dated: 17 November 2011

Name: Worcestershire County Council

Address: County Hall, Spetchley Road, Worcester WR5 2NP

Statutory framework

---

1. Worcestershire County 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 Worcestershire County Council and is referred to in this notice 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 he is the data controller.

2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1) (a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").

3. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in

conjunction with the Data Protection (Monetary Penalties)(Maximum Penalty and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

4. The data controller's [redacted] up to the age of 21. A member of staff working in the team accidentally clicked on an additional contact list and sent an email intended for internal use to 23 Ofsted registered care providers who consisted of fostering organisations, residential units, supported housing organisations, secure units and schools. Fortunately, all of the unintended recipients were used to handling sensitive personal data and operated under the data controller's protocols regarding the

handling of confidential data. Notwithstanding this, the nature of the error meant that there was a risk that the email could have gone to a wider external group who were not subject to any such requirements.

5. The email had two Excel spreadsheets [redacted]. All of the interpretable information on the spreadsheets was already known to the data subjects.

6. 14 of the 23 email addresses were generic contact points for receiving referrals and general correspondence. The other nine email addresses were personal. The member of staff immediately recognised her mistake and attempted an automatic recall of the emails. She also re-emailed and telephoned the unintended recipients to ask them to delete the original email. The data controller's Contracts Manager followed this up with another email requesting written confirmation that the email and attachments had been deleted and not disseminated any further.

7. 21 out of the 23 unintended recipients later confirmed deletion, one email was undeliverable and one email address was no longer used. The security breach was promptly escalated to senior management and an investigation was commenced culminating in a detailed report. All of the care providers referred to in the spreadsheets were informed of the security breach. However, [redacted] were not informed because the risk of further disclosure was assessed to be low and it would cause them undue distress.

8. The email and attached spreadsheets should have been sent to an internal "placement distribution" email group which is intended to appraise heads of service and senior managers (social care and finance) in the Children's Services Directorate about [redacted]. The data contained within the spreadsheets had been expanded over the years to meet the requests of managers with different requirements. It had been circulated on a weekly basis for the last 10 years without incident. Although the social care managers and finance officers did not need to have access to all of the information on the spreadsheets and could have obtained the information they required from other sources, the data controller adopted this method due to the ease of collection and distribution of

the information concerned. Essentially, the spreadsheet was used to double check that the information held by each department was correct.

9. Although attempts had previously been made to integrate this information within the secure social care database it had proved impossible to incorporate some of the data into the system. The Commissioner understands that specialist programming may provide a solution to this problem in the longer term. Following the security breach the spreadsheets are being held on a secure system which has now been developed to incorporate file sharing across children's services. Access to the spreadsheets is restricted to the relevant officers on a "need to know" basis and it is no longer necessary to email this data internally.

10. The data controller had some policies in place at the time of the security breach on how staff should deal with confidential information such as ensuring that emails are properly addressed. Centrally managed address lists were arranged to differentiate between internal and external address groups but lists created locally by employees did not. The Commissioner understands that the member of staff responsible for the security breach attended an induction course back in 2003 which may have involved some generalised data protection training but it was not compulsory at that time. The data controller's Information Security Policy also refers to the protection of internal information and clearly states that information should only be accessed by individuals on a "need to know" basis.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

---

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I of Schedule 1 to the Act, 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".

Paragraph 9 at Part II of Schedule 1 to the Act further provides 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 Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle in relation to all personal data with respect to which he is the data controller.

  In particular, the data controller had failed to take appropriate technical and organisational measures against unauthorised processing of personal data such as providing its employees with appropriate training, clearly differentiating between internal and external addresses in the central and local email distribution lists and considering an alternative means of handling the information such as holding it in a secure system that can only be accessed by members of staff who need to see it. The sensitive personal data on the spreadsheets could also have been minimised. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the harm that might result from such unauthorised processing and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress. Unauthorised confidential and sensitive personal data relating to [redacted] was unintentionally disclosed to 23 care providers due to the inappropriate technical and organisational measures taken by the data controller. The failure to take appropriate technical and organisational measures has the potential to cause substantial distress to individuals who would know or suspect that their confidential and sensitive personal data has been disclosed to people that have no right to know that information. The fact that the email and attached spreadsheets went to a relatively small group of recipients bound by confidentiality clauses was largely fortuitous. The nature of the error meant there was a risk that it could have gone to a wider external group who were not subject to any such requirements. Furthermore the individuals would be justifiably concerned that their data may have been further disclosed and possibly misused even if those concerns are not likely to materialise in this particular case. In this context it is important to bear in mind that many of the affected individuals are considered to be vulnerable.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because employees working in the data controller's [redacted] routinely dealt with confidential and sensitive personal data and managers should have realised the potential for human error in wrongly selecting drop down boxes when sending emails containing sensitive personal data, particularly when by employees who had limited training.

  In the circumstances, the data controller ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as providing its employees with appropriate training, clearly differentiating between internal and external addresses in the central and local email distribution lists, considering an alternative means of handling the information such as holding it in a secure system that can only be accessed by members of staff who need to see it and minimising the sensitive personal data in the spreadsheets.

  The risks of drop down boxes being wrongly selected are self evident and, in the Commissioner's view, widely known. Further it should have been obvious to the data controller who was routinely involved in dealing with [redacted] that such a contravention would be of a kind likely to cause substantial distress to the data subjects due to the nature of the data involved.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

---

Nature of the contravention

- Unauthorised confidential and sensitive personal data relating to [redacted] was unintentionally disclosed to 23 recipients
- Contravention of the Third Data Protection Principle in that excessive personal data was emailed on a weekly basis over a ten year period to potentially hundreds of staff internally who had no need to see it in breach of the data controller's own policy
- Contravention was serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- The contravention was of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Lack of appropriate training
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the unauthorised processing of personal data

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

---

Nature of the contravention

- To the Commissioner's knowledge the personal data involved in the security breach has not been further disseminated

Effect of the contravention

- The unintended recipients were all Ofsted registered care agencies operating under contracts and used to dealing with confidential data (although this was largely fortuitous)
- All of the unintended recipients have confirmed deletion
- All of the data subjects were already aware of the interpretable information in the spreadsheets

Behavioural issues

- A failed attempt was made to recall the email and attachments
- Voluntarily reported to Commissioner's office
- Detailed investigation report compiled
- All care providers mentioned in the attachments [redacted] were notified about the security breach.
- Substantial remedial action has now been taken

- Fully cooperative with Commissioner's office

Impact on the data controller

- Liability to pay monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund
- Significant impact on reputation of data controller as a result of this security breach

Other considerations

- The Third Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that excessive personal data was held on the spreadsheets

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to review the sending of confidential and sensitive personal data by email and to ensure either that more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of email

Notice of Intent

A Notice of Intent was served on the data controller dated 16 September 2011. The Commissioner received representations from the data controller in a letter from the Chief Executive dated 12 October 2011. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

The Commissioner considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £80,000 (Eighty thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 19 December 2011 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by 16 December2011 the Commissioner will reduce the monetary penalty by 20% to £64,000 (sixty four thousand pounds).

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

b. the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on 16 December 2011 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and
- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court or any sheriffdom in Scotland.

Dated the 17th day of November 2011

Signed: .....

David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the "Tribunal") against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be served on the Tribunal by 5pm on 16 December 2011 at the latest.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).