Data Protection Act 1998

Monetary Penalty Notice

Dated: 8 February 2012

Name: Cheshire East Council

Address: **Westfields, Middlewich Road, Sandbach, Cheshire CW11 1HZ**

Statutory framework

---

1. Cheshire East 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 on by Cheshire East 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 subject runs a Project which provides children with access to animals in the countryside. The Project's aim is to teach children to respect animals. On 23 March 2011, the Public Protection Unit ("PPU") was informed that the police had concerns about the motives of the data subject. The PPU formally referred the matter to the Local Authority Designated Officer (the "Officer"). The Officer agreed to monitor the situation in accordance with the "Potentially Dangerous

Person" process.

5. On 8 April 2011, the data controller identified wider child protection concerns in relation to the data subject and sought internal legal advice about sharing those concerns with agencies that use the Project. On 12 April 2011, the Officer attended a multi-agency "Potentially Dangerous Persons" meeting. At the meeting it was agreed that the Officer should inform the co-ordinator for the voluntary sector about their concerns.

6. On 14 April 2011, the Officer sent an email to the Assistant Officer attaching the legal advice about disclosing the information together with instructions from the "Potentially Dangerous Persons" meeting. The Assistant Officer was asked to contact the voluntary sector co-ordinator to progress the instructions from the meeting. The Assistant Officer was not informed which agencies should be contacted or how these instructions should be acted on by the voluntary sector co-ordinator. In addition, the Assistant Officer had not received any data protection training.

7. On 3 May 2011, the Assistant Officer sent an email to the voluntary sector co-ordinator at her personal web email address in breach of the data controller's policy that secure means must be used when sending data to external recipients. However, the Assistant Officer could not use the secure government email network because the voluntary sector co-ordinator did not have an appropriate email account. Further, she could not use the local secure email system because this would have prevented the information in the email from being further disseminated by the voluntary sector co-ordinator.

8. The email identified the data subject by name and an alleged alias and referred to the data subject as the person who runs the Project. The email also informed the voluntary sector co-ordinator that the police had significant child protection concerns about the data subject and that he was not an appropriate person to work with children and young people. The email then asked the voluntary sector co-ordinator to inform voluntary agencies that provided services to children and young people within her network not to use the Project. The voluntary sector co-ordinator then forwarded the same email to 100 intended recipients who interpreted this to mean that they too should forward the email to voluntary organisations as appropriate. The email was therefore sent to a further 180 unintended recipients.

9. Following the security breach, the data controller attempted to recall the emails that were forwarded to the unintended recipients, although the majority are still unidentified. The data controller also sent an

email to the intended recipients asking them to delete the original email. The data controller has confirmed that approximately 57% of the intended recipients have deleted the email. In future, it is proposed that the Officer will decide whether it is necessary to share such information with other agencies and, if so, how that information should be disclosed. Further, that sensitive personal data will be kept to a minimum, password protected and communicated via a secure email account. The Assistant Officer has now received management advice in relation to this matter and appropriate data protection training

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 the Assistant Officer with appropriate data protection training and support, carrying out a risk assessment before disclosing sensitive personal data by email and

considering a more secure means of transmission. 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 damage or substantial distress. Unauthorised and highly sensitive personal data relating to one data subject was disclosed to 180 unintended recipients 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 the data subject who is aware that highly sensitive personal data has been disclosed to a large number of people who have no right to see that information. The contravention is also likely to cause substantial damage to the data subject whose livelihood has been jeopardised by the unauthorised disclosure. Furthermore, the data subject would be justifiably concerned that his data may be further disclosed and possibly misused even if those concerns do not actually materialise.

- 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 damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because the Officer and Assistant Officer working with the PPU might deal with highly sensitive personal data from time to time. Therefore the data controller should have identified the potential risk of emails containing highly sensitive personal data being sent to a personal web email address, particularly when the Assistant Officer concerned had not received any data protection training and support.

  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 the Assistant Officer with appropriate data protection training and support, carrying out a risk assessment before disclosing sensitive personal data by email and considering a more secure means of transmission.

  Further it should have been obvious to the data controller whose staff working with the PPU might deal with highly sensitive personal data from time to time as part of the "Potentially Dangerous Person" process, that such a contravention would be of a kind likely to cause

substantial damage or substantial distress to the data subject 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 and highly sensitive personal data relating to one individual was disclosed to 180 unintended recipients
- Contravention was serious because of the highly sensitive nature of the personal data

Effect of the contravention

- Highly sensitive personal data relating to one individual could still be available to third parties
- The individual was compelled to refute the allegations in the local press
- The contravention was of a kind likely to cause substantial damage or substantial distress to the data subject

Behavioural issues

- Lack of appropriate data protection training and support
- 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

- First time that personal data of this nature had to be disclosed to the voluntary sector co-ordinator

Effect of the contravention

- Attempts were made to recall the email and prevent further dissemination
- 57% of the intended recipients have confirmed that they deleted the information

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data controller apologised to individual affected
- Substantial remedial action will be 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 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 handling of sensitive personal data and to ensure that 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 21 December 2011. The Commissioner received a letter from Legal Services dated 27 January 2012 informing him that the data controller did not wish to make any representations in relation to the notice of intent. The Commissioner has now 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 8 March 2012 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 7 March 2012 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 7 March 2012 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 8th day of February 2012

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 7 March 2012 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)).