Devon County Council

CP1329-16

OJEU REF – 2017/S 042-076945

Data Protection: What you need to know Guide

CP1329–16 Supporting Independence.

(Appendix G)

Supporting Independence

Appendix G Data Protection – What you need to know Guide

1.0 Introduction

As part of this contract, Devon County Council will be providing you with a limited amount of relevant personal data, to enable you to deliver unregulated support to Devon residents. Personal data is information about living, identifiable individuals.

The Data Protection Act 1998 sets out the legal obligations of organisations who process personal data. The processing of personal data covers all aspects of handling and using the data, including, but not limited to, obtaining, holding, storing, sharing, and destroying the data.

As Data Controller of the information you will receive, Devon County Council is legally required to ensure that you process this information securely on behalf of the Council. By processing personal data securely, you will minimise the risk that it is accidentally lost, or accessed inappropriately.

To ensure that you process the information that you receive securely, you must ensure that you have the following organisational arrangements in place:

- A Data Protection policy which has been read and signed by all employees who handle personal data on behalf of Devon County Council
- Data Protection Training which has been delivered to all employees who handle personal data on behalf of Devon County Council
- Provide a secure office environment where personal data will be stored and processed
- Provide all staff who carry personal data out of the office with a secure method of transporting that data
- Practical information security guidance which is freely available to staff
- If processing personal data electronically, technical arrangements which sufficiently protect personal data from unauthorised access and from accidental loss, damage or destruction
- A process for investigating suspected Data Protection breaches and a nominated officer who will liaise with Devon County Council in the event of a breach involving our data
- A nominated Data Protection lead who will be responsible for overseeing your organisation's compliance with the above

2.0 What must your Data Protection Policy include?

It is essential that your Data Protection Policy contains the following:

- A requirement for all staff to abide by the Data Protection training at all times, when handling Devon County Council data
- Prohibits staff from processing personal data outside the strict requirements of their job role

- Confirms that any deliberate or reckless breach of the Data Protection policy by an employee may result in disciplinary action, which could lead to dismissal
- Identifies the person in your organisation who is responsible for overseeing compliance with the policy
- Identifies the person/team in your organisation who should be notified in the event that a Data Protection breach is suspected
- A requirement for all staff to report any suspected Data Protection breaches to the nominated person within your organisation
- A procedure for investigating suspected Data Protection breaches and notifying Devon County Council in the event that the breach involves Devon County Council information

3.0 What must your Data Protection training include?

Data Protection training must be mandatory for all staff who process personal data on behalf of Devon County Council.

Your Data Protection training must provide staff with the necessary practical knowledge required to keep personal data secure. In particular, the following points must be included:

<u>Emailing Personal Data</u>

- Before sending personal or confidential information by email, always double-check that recipient names, email addresses, and attachments are correct.
- Do not forward unnecessary email trails and always double-check that the content is appropriate.
- Limit the amount of personal data that you send to only that which is necessary.
- When emailing more than one recipient, use the 'Bcc' function to hide recipients' identities, unless there is a legitimate reason why the names and email addresses of recipients would need to be shared.
- When sending particularly sensitive information, consider asking a colleague to undertake the above checks for you (known as a "peer check")

<u>Posting Personal Data</u>

- Before sending personal data by post, always double-check that you are sending the information to the correct recipient and that you have addressed the envelope fully and correctly.
- Always check that any documents you are sending have not been mixed up with other information.

- Clearly mark the envelope or parcel “private and confidential” and/or “to be opened by addressee only”, and include a return address.
- When sending particularly sensitive information, consider asking a colleague to undertake the above checks for you (known as a “peer check”)

Office Security

- Lock your computer screen when you leave your desk.
- Ensure that visitors are accompanied at all times whilst in the building.
- Destroy or dispose of paper files securely
- Do not print personal data unless absolutely necessary and do not leave the printer unattended whilst printing personal data.
- Keep your desk clear of any papers besides those required at a particular time.
- All personal or confidential information held in any form; e.g., paper, CD, memory stick, etc. must be locked away when unattended.

Carrying Personal Data Off-Site

- Never take more personal data out of the office than is necessary.
- Carry paper files in a locked briefcase or in a folder or bag that can be securely closed or zipped up. Ensure that the briefcase/folder/bag contains your name and contact details.
- Never leave paper files, laptops or mobile phones unattended, even for a short time. Lock them away or keep them with you.
- Count how many files you have before you set off and check that you have the same number of files prior to leaving all destinations.

Viruses, SPAM and Suspicious Emails

Email accounts around the world are bombarded with millions of rogue emails every day, in an attempt by hackers to gain access to confidential systems and information. Staff must learn to recognise these and deal with them accordingly.

If you receive a suspicious email, do not open it, or click on any attachments or links. Doing so could infect our network/systems with a virus and lead to a catastrophic loss of information and disruption to

business. Instead, you must permanently delete any suspicious emails you receive, without opening them.

If an email looks plausible but at the same time feels a little odd or suspicious, mentions unexpected invoices, faxes, or encourages you to 'click here' urgently, then it is likely to contain a virus.

The email itself may look as if it comes from a genuine source. Fake emails often (but not always) display some of the following characteristics:

- The sender's email address is different from the trusted organisation's website address.
- The email is sent from a completely different address or a free webmail address.
- The email does not use your proper name, but uses a non-specific greeting such as "Dear Employee."
- A sense of urgency; for example, the threat that unless you act immediately your account may be closed.
- A prominent website link. These can be forged or seem very similar to the proper address, but even a single character's difference means a different website.
- A request for personal information such as username, password or bank details.
- You weren't expecting to get an email from the organisation that appears to have sent it.
- The entire text of the email is contained within an image rather than the usual text format. The image contains an embedded link to a bogus site.

Accessing Personal Data Appropriately

Staff must be aware that access to personal data is only permitted for the purposes of allowing a staff member to perform their job role. It may be an offence under the Data Protection Act and/or the Computer Misuse Act if a member of staff deliberately accesses personal data outside the requirements of their employment.

Reporting a Suspected Data Protection Breach

If you suspect that personal data has been inappropriately accessed, shared or disclosed, either deliberately or by mistake, you must report this to:

[*contact details of nominated person/team within your organisation with responsibility for investigating suspected Data Protection breaches*]

4.0 How can you provide a secure office environment?

Any offices or buildings which are used to store or process Devon County Council information must provide an adequate level of security. This includes restricted access to areas where our information is

held (for example swipe card access or keys which are only held by those staff members who require access).

Devon County Council information must be locked away when not in use, and cabinets/cupboards etc, must only be accessible to staff who are permitted to process our information.

You organisation must provide arrangements for the secure disposal of personal data, both electronic and paper format. Once personal data has been disposed, it must not be possible to then recover that data. An example of secure disposal would be the shredding of paper documents.

5.0 What equipment must staff be provided with for transporting data outside of the office?

Depending on the type of service you will be providing, there may be a requirement for staff to take personal data away from your office base in order to deliver the service. This is permissible, provided that staff are fully trained and have been provided with a secure means of transporting the information. All staff who carry paper files, or electrical items which contain personal data, out of the office, must be provided with a lockable briefcase, or a folder or bag that can be securely closed or zipped up. Briefcases/folders/bags must contain your organisation's contact details.

6.0 What guidance must be made freely available to staff?

Please see section 3.0. The training material should be freely available to staff electronically (e.g., staff intranet pages) or on posters displayed in the office. In addition, we would expect staff to be regularly reminded of this guidance in staff supervision sessions, appraisals and via any relevant newsletters/staff bulletins. This training is mandatory for any staff who handle Devon County Council information and refresher training must be provided on an annual basis.

7.0 What technical arrangements must you have in place?

You must ensure that access to Devon County Council information is restricted, so that only employees who need it to enable the contracted service to be delivered are able to access the information.

If you will be processing Devon County Council's information electronically, you must ensure that you are compliant with the requirements of the government's Small Businesses: What you need to know about Cyber Security. This will help protect you from cyber threats such as viruses.

8.0 What must you do if you suspect that a Data Protection breach involving Devon County Council data has occurred?

If you suspect that a Data Protection breach involving Devon County Council data has occurred, you must notify the Council immediately, by emailing keepdevonsdatasafe@devon.gov.uk, or by phoning 01392383000 and asking for the "Information Governance Team".

We will ask you to provide us with a report detailing the following:

- What personal data was involved
- In what way the personal data was inappropriately processed and/or who it was disclosed to
- How the incident occurred
- What you intend to do in order to prevent a similar incident from occurring in future

If requested, you must be able to provide evidence to Devon County Council that all staff members handling our information have signed your Data Protection policy and received your Data Protection training.