3 SAFE AND SECURE TRANSFER OF INFORMATION

1 Purpose

All signatories to Personal Information Sharing Agreements (PISA) prepared under the WiSC must take appropriate steps to ensure that the physical and electronic exchange and storage of personal and sensitive information shared between them is safe and secure. A template PISA is available for use within these resource notes.

This guidance provides advice on how to adhere to the sixth principle of the General Data Protection Regulation 2016 - which is to ensure data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Understanding the risks of information sharing, and agreeing how to manage them should initially be considered in a Data Protection Impact Assessment (DPIA), before a PISA is completed. For guidance on how to complete a DPIA, see resource note 5 – 'Data Protection Impact Assessments'.

2 Definitions

The sharing of information requires it to be transferred from one source or organisation to another for processing. Personal and special category information can be kept in hard copy or electronic formats and shared in a number of different ways. Different formats of information present different risks to the safe and secure transfer from one partner or organisation to another.

In order to ensure the safe transfer or sharing of information, the risks to loss or interference to the information during and after its transfer need to be understood and managed.

In terms of roles and responsibilities, the organisation that originally collected the personal and special category data from individuals is the Data Controller. It is the Data Controller who will be held accountable for any loss, damage or destruction to the information by the affected data subjects and/or the ICO.

3 Different ways of sharing information

Information can be shared between partners in a number of different ways:

- in hard copy – the transfer of paper files from one office to another, internal and external post, printed case file notes shared at meetings;
- electronically – through emails, by fax, using mobile and removable portable devices, through shared information systems such as the Single View project;
- verbally – on the telephone, at face to face meetings.

All of these present different information security risks that must be considered and mitigated against before a PISA is agreed.

4 Risks of sharing information safely

Below are just a few examples of information security risks but this list is by no means exhaustive:

- paper records gest lost or stolen while in transit or when left unsecured in offices;
- post sent to the wrong person, wrong organisation, wrong department or address;
- confidential case file notes taken away from meetings, left in meeting rooms or left in unattended and unlocked bags;

- emails sent to the wrong recipients;
- faxes sent to the wrong fax number.

Mobile working increases the likelihood of some information security risks:

- USB sticks, mobile phones, ipads, laptops lost or stolen;
- personal details shared over the phone in reception areas and other public places;
- discussions about clients held in the presence of visitors not normally in the safe office environment;
- shoulder surfing (looking over your shoulder at the information on your laptop, smart phone or tablet) may take place in public places.

One of the key risks for information sharing between partners will be unauthorised or inappropriate access to shared information systems.

5 Steps to reduce the risks

Initially, only collect and share the minimum information required for the intended purpose – as required in the third Data Protection principle. This will help reduce the impact of any data losses. Some examples for managing risks are outlined below:

Physical and technical security

All partners of a PISA should be comfortable with each other's physical and technical security measures. Look for ICT access policies, clear desk policies, secure office environments, restricted access arrangements to buildings and offices and ICT equipment.

Post

If sharing information by post – double bag/envelope (and sign over the seals), and send the information by secure method such as special delivery.

Alternatively, arrange for personal collection of files by an identifiable person but have agreed rules about the actual transit i.e. go straight to the destination - no deviation for lunch or shopping trips enroute, transport the files in the boot of the car.

Introduce meeting rules where personal and sensitive information is to be shared such as agreement that information will only be handed out at the meeting and all copies will be collected at the end of the meeting.

Emails

Use email encryption tools and/or secure email addresses for transferring information. Check with your organisation's ICT department and record the agreed transit arrangements in the PISA.

For general email use, switch off auto-complete to reduce the risk of sending information to the wrong recipient.

Use BCC to protect individual's anonymity, take care with use of 'reply to all', use reference numbers rather names in the subject line and review history strings before hitting 'send'.

3 SAFE AND SECURE TRANSFER OF INFORMATION

Mobile devices

Individual organisations should have mobile working policies. All partners to a PISA should be aware of whether the information is going to be held on mobile devices, and should be comfortable that adequate encryption and password access controls are in place to protect the information.

Mobile working

Check your surroundings, make sure no one is 'shoulder surfing'. Use a privacy screen for your device or position yourself appropriately.

Ensure no one is listening to your conversation. Make sure no one is posing as a person who can be trusted to obtain information - known as "blagging".

6 Loss of data

There will always be a risk of interference with or loss of information and in some circumstances the consequences can be severe for the affected individual and the Data Controller. However, if robust steps have been taken to protect information security and those engaged in the exchange and transfer of it are clear on the requirements, the likelihood of a financial penalty imposed by the ICO are reduced.

For guidance on how to manage a data breach, please refer to resource note 8 - 'Data Breach Management'.