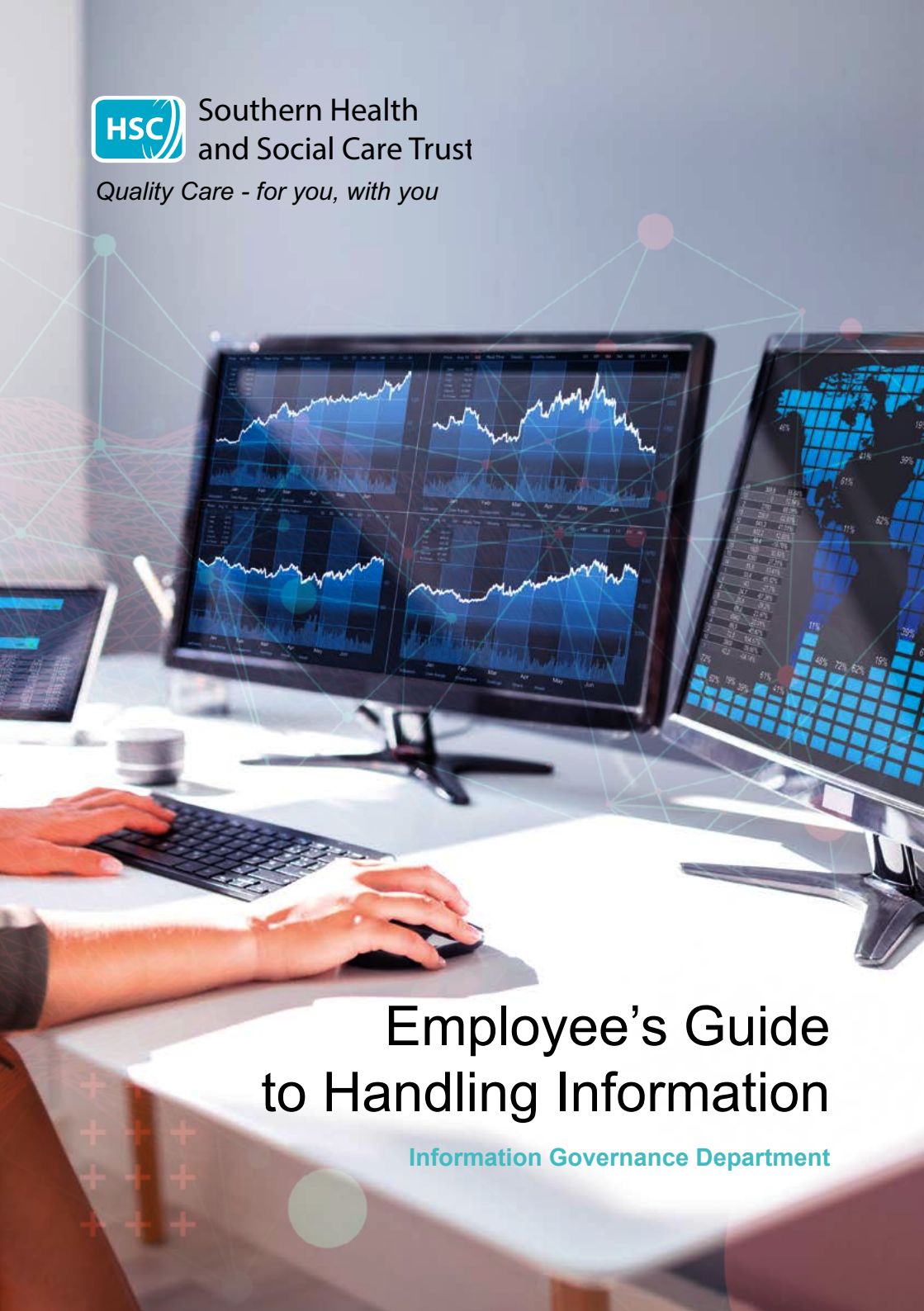
Southern Health and Social Care Trust

Quality Care - for you, with you



Employee's Guide to Handling Information

Information Governance Department

Contents

Introduction

Southern Health and Social Care Trust needs to collect and use personal information about people in order to operate. All individual staff members who access or use personal information must do so responsibly and in line with the legal requirements - the General Data Protection Regulation. (GDPR)

FACT:

The Information Commissioners Office (ICO) has the power to fine the organisation a maximum of €20 million for breaching the GDPR

Failure by a staff member to comply with these requirements could result in disciplinary action, involvement of the PSNI and in some cases, lead to potential criminal proceedings.

Data breaches may result in the Trust facing a range of measures by the Information Commissioner's Office (ICO) up to and including a fine of €20 million Euros! Understanding the relevant Trust policies, asking the right people for advice and taking personal responsibility for how you handle personal information will help you to get it right and comply with Data Protection requirements within your day to day role in the Trust.

[Read the Trust's Policy on Data Protection]

What is the GDPR

It is the law and protects personal privacy and upholds individuals' rights.

Does the GDPR affect me?

Yes! The GDPR affects everyone who handles or has access to information about individuals. The GDPR also gives rights to the people the information is about. By law, everyone in the workplace must follow the rules set out in the GDPR and help to protect individuals' rights.

What are my responsibilities?

The GDPR helps make sure that information held on computer based systems and paper-based record systems is managed properly. You must protect personal information by following the 7 Principles of the GDPR. **All staff** must ensure they undertake Data Protection training and keep this updated, as per Trust's **eLearning Policy**.

The seven principles of the GDPR

The GDPR is based on 7 principles or rules for 'good information handling'

In summary, the data must be:

a. processed lawfully, fairly and in a transparent manner,

b. collected for specified, explicit and legitimate purposes,

c. adequate, relevant and limited to what is necessary,

d. accurate and where necessary kept up to date,

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed, and

f. processed in a manner that ensures appropriate security of the personal data.

'Accountability' is often known as the 7th Principle of the GDPR

Accountability

The Trust has to demonstrate why it uses personal data for each different purpose. **Accountability is central to GDPR**. Knowing what data you have and why you use it is important in demonstrating accountability.

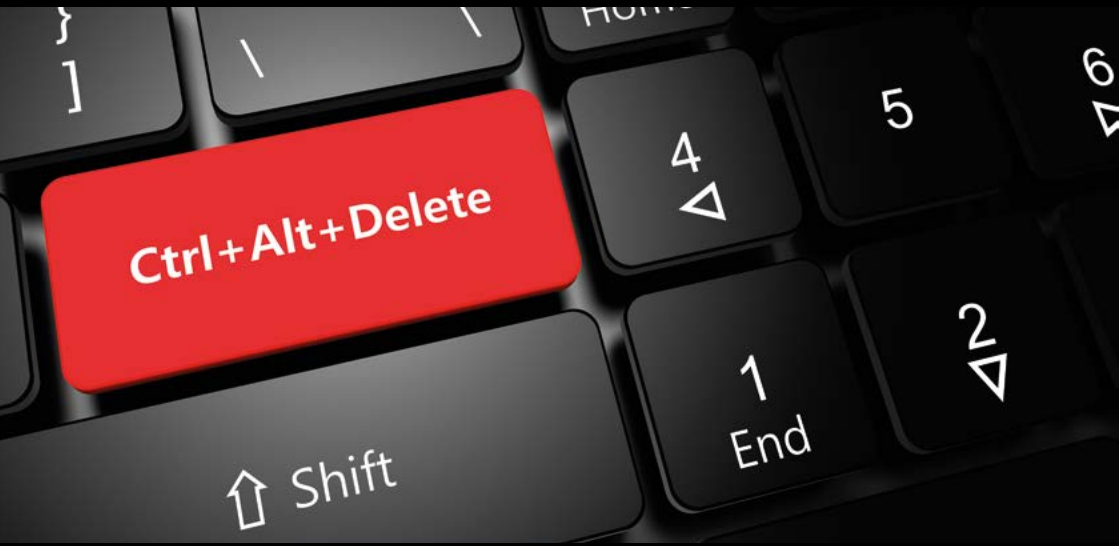
Keeping Personal Information Secure

Personal or sensitive information should always be kept secure, whether paper or electronically held records. Do not leave records unattended in areas where the public can access them.

If accessing electronic records on computer systems, angle the screen away to keep the information private.

Don't forget to activate your screen saver as soon as you leave your work station.

Medical staff who use **addressograph** labels for recording Surgical logs should complete this work in the work environment as soon as practical and place the labels into the confidential waste when the log books have been updated.



FACT:
GP Receptionist fined by the ICO for looking up records on ex-husbands' new wife

Use of computer systems

Using Trust systems gives you access to a lot of sensitive information, including personal information about many individuals. Always log onto systems using your own username and password but do not access information unless you have a legitimate business reason for doing so.

Your login details for Trust systems must not be disclosed or shared with anyone else – it is your responsibility to keep them private!

There are easy, secure ways to share your emails and files with another staff member using their own account.

Accessing records

Remember it is a criminal offence to access systems for your own purposes, for example, looking up a neighbor or relative's test results, or your own! This can result in a criminal prosecution, a fine, loss of your job and a criminal record!

Cyber Security

Whilst technical controls are in place to help protect the network and information as much as possible from malicious files or access, we also need everyone to be extra careful!

Be especially cautious of suspicious emails or links to external websites. Even opening these emails or links can create problems without your knowledge and this can lead to the network, systems or information being compromised or exposed to criminals.

[Health data is highly sought after!]

Stay alert and report any other suspicious activity to ICT Service Desk. Email any example to: spam@southerntrust.hscni.net

The faster it is reported, the faster it can be dealt with.

Many non-traditional devices are now being used to process or access information, including medical devices.

Make sure you follow your department protocols for safe handling of information when using these devices, particularly if you have to transfer information between the device and Trust systems or network storage.

Be aware that medical devices have the potential to be a cyber security risk. Check with your Line Manager or systems' manager in the first instance if you are unsure.

Emailing

Remember that information security rules apply to the use of email as well. When emailing sensitive or personal information to organisations external to the Trust, and who are not part of the wider-HSCNI protected network, the data will be sent over the public internet. Encryption is a way to secure the information until it reaches your intended recipient – so encrypt all emails that contain personal or sensitive information before sending.

Search the Information Governance SharePoint site for guidance on Encryption Options, including 'Transferring Information Securely' leaflet.

Personal or sensitive information should never be emailed to your home email account! If you need to do work at home, request Staff Secure Remote Access. This solution has been specifically designed to provide you with secure access to your Trust files, emails and systems from home.

Before sending Trust email:

- Always double-check you have selected the correct email address/contact
- Don't REPLY ALL - make sure you only include those who need to get the information
- Use BCC to "blind copy" someone into an email. The purpose of BCC ensures email of addresses of other (particularly personal email addresses) are protected and not shared inappropriately or unnecessarily with others.
- Consider setting your email to delay outgoing messages. This will give you the opportunity to reflect on the content, amend errors, encrypt, or reconsider if the message should be sent at all.

Social Media & Apps

Social media offers a great way to communicate with friends, colleagues and other people but there are risks and issues relating to personal data, for both the individual and the Trust.

If you can be identified as a member of Trust staff when using social media such as Facebook or Twitter, you must not mention any information relating to a patient, client, colleague or the Trust. Always act in a professional and responsible way when using social media.

[Read the Trust's Social Media Policy!]

Social Media technologies & Apps provide many opportunities to improve the way we communicate reach out and interact with others.

However there are risks associated with the use of these technologies and apps eg WhatsApp, Facebook, Twitter and particularly with regards to personal information. Always ensure you follow your department's protocols on the safe and acceptable use of these technologies, including what apps are authorised to be used for Trust business.

Secure Disposal

Electronic devices that are used to process personal or sensitive information must be securely erased before disposal or re-use. This includes devices like PC's, laptops, mobile phones etc. and even some printers.

Using an authorised contractor means that the data is securely erased and therefore sensitive information will be kept private and not end up in the wrong hands or available on the internet!

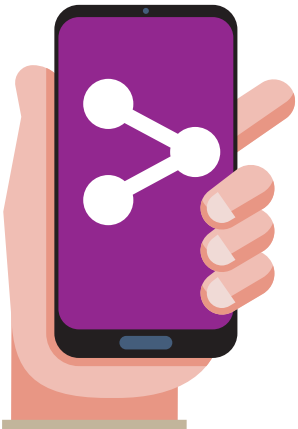
Contact ICT Service Desk to organise equipment for secure disposal. **Never place in waste bins or skips!**

Telephone Calls

Depending on your role, you may be required to handle enquiries or requests for personal information. Did you know that you can breach the GDPR if you give out information to someone who is not entitled to it?

Always check the person's identity first if you are unsure about giving out the information or suggest they write in for it.

Don't let yourself be bullied or tricked into giving out the information – seek assistance from your line Manager.



On those occasions where you need to leave a telephone message for someone on their home or mobile phone, leave your **direct dial** contact number – not the message itself. Remember, the message could be picked up by someone else.

Transporting records

Did you know that records are most at risk when being transported outside the organisation? ‘Records’ also include personal work diaries, reports and doctors’ correspondence, not just patient files.

On those occasions where you must take records home as part of your job, put them in a ‘secure vessel’ (container or bag), place in the boot of the car and remove the records into your home on arrival. Beware ! Never be tempted to leave records in your car overnight or leave them where they are visible – even for a short period.

[Read the Trust’s Transportation of Records Policy]

Retention and Disposal of records

The Trust has a legal obligation to manage, retain and destroy its records in line with the Department of Health guidelines. Therefore all records within the Trust should be retained and destroyed in accordance with the ***Department of Health’s Good Management and Good Records Retention and Disposal Schedule***.

Guidance on the retention and disposal of records can be found on the Information Governance Sharepoint Page.

How we handle others information

The Trust has a Privacy Notice on our website to inform patients/clients on how we use their personal information.

Posting Personal Information

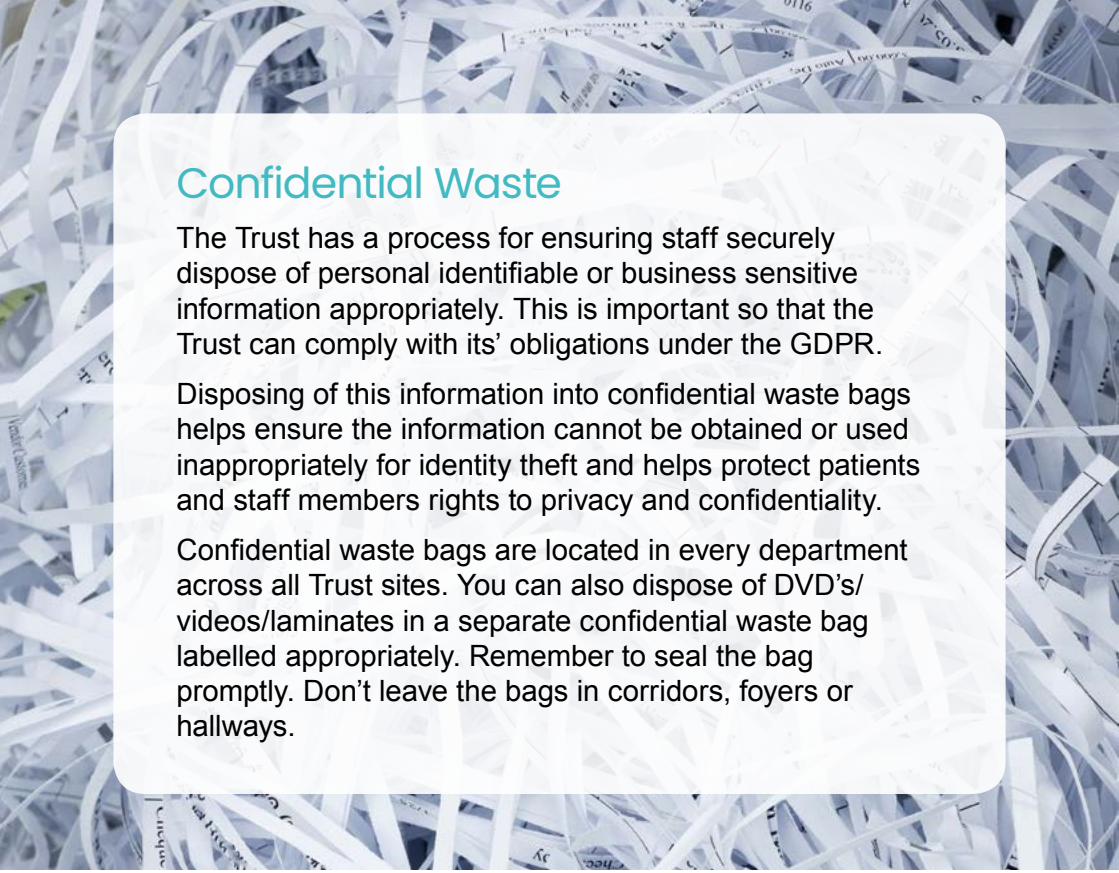
As part of your job you may need to send personal or sensitive information by post. Always write the full address. Do do not be tempted to use abbreviations for Trust facilities as this can be confusing. Do you know what SHWTC or F&CC stands for? – Not everyone does!

If you post sensitive information outside the Trust use an appropriate return address on the back of the envelope – this allows it to be returned.

Ensure all addresses have a postcode on the envelope, including those generated directly from a system.

Any attached documents should be double checked to ensure they match the intended recipient.

Where feasible, mis-sent patient/client information should be retrieved by the Service concerned. If this is not possible, send a stamped addressed envelope so the information can be returned to the Trust the recipient should not be asked to destroy the information!



Confidential Waste

The Trust has a process for ensuring staff securely dispose of personal identifiable or business sensitive information appropriately. This is important so that the Trust can comply with its' obligations under the GDPR.

Disposing of this information into confidential waste bags helps ensure the information cannot be obtained or used inappropriately for identity theft and helps protect patients and staff members rights to privacy and confidentiality.

Confidential waste bags are located in every department across all Trust sites. You can also dispose of DVD's/ videos/laminates in a separate confidential waste bag labelled appropriately. Remember to seal the bag promptly. Don't leave the bags in corridors, foyers or hallways.

Reporting Incidents (Data Breaches)

If you are aware or suspect that an incident (data breach) has occurred, report it to your Line Manager immediately and complete a Trust Datix form. The Information Governance Team must be contacted in case the incident has to be notified to the ICO.

It is important the incident is appropriately dealt with as soon as possible, in order to minimize any potential distress to the people concerned.

Remember that reportable breaches must be reported to the ICO (by the Head of Service to the Information Governance Department) within 72 hours of discovery of the breach.

Subject Access Requests

Under the GDPR an individual has the right of access to personal Information that we hold about them. Individuals can apply for records under the 'Subject Access Request' process.

Remember that under the GDPR the Trust must also accept requests both verbally and in writing (including email).

Freedom of Information

The Freedom of Information (FOI) Act 2000 makes it easier for people to get information about the Trust.

This law, which came into force on 1st January 2005, means that anyone, anywhere can ask for information we hold. FOI relates to Corporate, not personal information.

Under the FOI Act 2000, the Southern Health and Social Care Trust is legally committed to providing timely and accessible information to the public and responding to reasonable requests for information. There are no time limits on how far back anyone can gain access to information, as long as we hold it on record.

Good Information Handling in Your Job - Your Five a Day!

1. Keep it secure

When handling personal or sensitive information, keep it secure - both during and after use. Never leave records such as patient files, personal work diaries or appointment letters where they can be accessed or removed inappropriately.

2. A place for everything and everything in its' place

If you write personal identifiable details (name, address, DOB, treatment etc) onto loose sheets or paper, this information belongs in the patient record or should be placed in the confidential waste when no longer needed (as appropriate).

Loose sheets can be easily dropped or lost. Would you like your sensitive information picked up by a member of the public?

If you discover personal information has been mis-filed into the wrong file, please notify your line Manager.

3. Should I hand this information over?

Think before handing over personal or sensitive information to anyone. Only staff who need the information for the purpose of their work should have access to it. Requests from patients/clients or staff for information the Trust holds relating to them must be directed to the Information Governance Team.

4. It only takes a moment

Some roles may involve handing a patient/ client their own record, such as Antenatal Clinic appointments.

Always check it is the right file for the right patient. It only takes a moment and can avoid unnecessary distress to a patient.

5. Keep it current

Where possible, check patient/client address and contact number has not changed. Personal information that is incorrect, inaccurate or out of date can result in delays to patient appointments or to sensitive information being opened by the wrong person.

For more information visit the Information Governance Sharepoint Site.

Notes

Southern Health and Social Care Trust

Quality Care - for you, with you

For more information contact:

Information Governance
Ferndale House
Gilford
Tel: 028 37 561458
Email: Foi.team@Southerntrust.hscni.net

A special thanks to the Information Governance Team in the Belfast HSC Trust who developed this leaflet.