

# Data Security and Protection Policy

---

## Overview

### What is this policy?

This policy sets out what we think about data security and protection and how we keep data safe. It's published on our website so anyone can see it, and it applies to everyone – people who work for us and people who use our services.

Guidance about how the people who work for us should act is in the blue 'Resources' boxes throughout this document, that only they can access.

### When do we use this policy?

We use this policy when we are in contact with data and information at any stage:

- before we use or make records
- while we are working with people on a record
- when we are closing or archiving records and when something goes wrong.

Use this policy with our other policies about how we look after information: Privacy, Sharing and Confidentiality and Information Rights. You can find them on our website, or if you work for us, you can access them through our shared drives.

### What's included in this policy?

#### [Overview](#)

[What is this policy?](#)

[When do we use this policy?](#)

[What's included in this policy?](#)

## What is data security and protection?

Records management – know where the data is

Data protection – think about keeping data safe

Data security – how we keep data safe

Further reading: Data security and protection (links to other sites)

## Looking after records (record management)

Know what a record is

Know why we keep records

Look after records at all times

Keep records updated and complete

Resources: Looking after records

## Keeping data secure

Lock records away: Physical security

Some examples of how we keep physical records and equipment safe are that we:

Use safe software: Digital security

Some examples of how we keep data safe on the computer are that we:

Have a secure attitude: Security thinking

Some examples of how we use our thinking to keep data safe are that we:

Resources: Keeping data secure

IT Policies:

## Know what you need to do

Resources: Know your duty

## Follow the Law

Use the Data Protection Principles:

Use data fairly, clearly and in line with the law

Data about service users

Data about people who are working on our behalf

[Be responsible for our data](#)

[Only use and share what we need to do our jobs](#)

[Know what data we have and where it goes](#)

[Resources: Follow the law](#)

This policy was last updated: Sept 2020

This policy will next be updated: Sept 2021

# What is data security and protection?

## Records management – know where the data is

We hold all sorts of data about a whole range of things so that we can do our jobs and help the people we work with to achieve their goals. Lots of this information is held in records about people's health and personal life, so it requires extra care. People trust us to look after their data (kept as records) and use it responsibly. We sometimes call this records management.

## Data protection – think about keeping data safe

Data protection is all about our approach to treating the information we are trusted with wisely when it is in our care and when we move it around. We also call this good Information Governance (IG). We use the law and other resources (like the [NHS Data Security & Protection Toolkit](#)) to help us protect the data we have.

## Data security – how we keep data safe

Data security is about the ways we take care of our data and keep it safe (confidentiality), making sure that we can trust the data we have (integrity) and that it is easy to find and use when we need it (availability). Where our data is held on computers, data security is closely linked with good IT practices.

We trust all the people who work for us to follow their training, our guidance and the law to keep data safe. Some of them have special IG roles to help us interpret the law and guidance and put it into practice.

### → Further reading: Data security and protection (links to other sites)

- [Data Protection Act \(DPA\)](#) 2018
- [General Data Protection Regulation \(GDPR\)](#) 2016
- [National Data Guardian \(NDG\)](#) reports and recommendations
- [NHS Data Security & Protection Toolkit](#)
- [Information Commissioner's Office \(ICO\)](#) papers
- [Caldicott Guardian](#) reports and principles

- [Information Governance Alliance \(IGA\) – Records Management Code of Practice for Health and Social Care 2016](#)
- [ISO \(the International Organisation for Standardisation\) IT Information Security standards](#)
- [The National Archives](#) guidance

# Looking after records (record management)

## Know what a record is

We keep records about things like our money, buildings, services and people who work for us as well as the people who use our services. Records can be kept in lots of different ways; such as computer files, papers, video, photos, sound recordings and text messages.

Our database records are a “single version of the truth”. This means that we keep one record per person updated with everything that’s happened in a safe place. That way we can find everything when we need it.

## Know why we keep records

- To keep people safe
- So we can remember what we’ve talked about
- So we can make good decisions from all the information available
- So we can show how we’ve come to those decisions and the work we have done
- To learn from successes and mistakes
- Because the law says we must

## Look after records at all times

We look after records from when they are first made or given to us. When the record stops – for example when someone no longer needs a service – we close it as soon as we can. We keep looking after the closed record for as long as we need to keep it (in archive), and then make sure it is securely destroyed. We use the latest guidance for healthcare organisations to help us decide when to delete or destroy the record.

## Keep records updated and complete

We add to our records whenever anything happens (within 48 hours) so that they are always up to date. We check that the data is correct with the person who knows best – usually the person that the record is about. We try to keep everything in one place (a database) and make a note if we need to move or keep something elsewhere.

## → Resources: Looking after records

- [How to...look after records](#)
- [How to...archiving and retention](#)
- [How to...look after audio and video recordings](#)
- [Case Management Policy and S.O.P. \(DQ163\)](#)
- Keeping Information Safe training ([Loop](#))
- [Information Governance Alliance \(IGA\) – Records Management Code of Practice for Health and Social Care 2016](#)
- [The National Archives](#) guidance

# Keeping data secure

We need to use and share information so that we can do our jobs. It's really important that records are up to date and seen by the right people in the safest way possible. We keep most of our records on our computer systems, which have some built-in security measures but also rely on users to keep the data safe. If we need to use paper records, we must keep them safe using different methods. We always need to use our common sense to keep data safe, as well as following our guidance and policies.

## Lock records away: Physical security

### **We keep physical records and equipment safe by:**

- Keeping our desks clear and screens locked when we're away from them, even if it's just for a few minutes while we're making a cup of tea
- Turning our screens away from other people or windows
- Soundproofing rooms that we use to see people or moving to a private area to take a sensitive phone call
- Using locks, keypads and alarms on our offices, and making sure doors are fully closed
- Having separate areas at our services for the people who work for us and the people who use our services
- Locking records away when we're not using them or if we have to move them
- Keeping track of where files are at all times (for example using a sign in/out sheet if we have to take files out of the office)
- Shredding paper copies when we don't need them using a cross-shredder or an approved service

## Use safe software: Digital security

### **We keep data safe on the computer by:**

- Using our own unique usernames and passwords to log in to our computers and databases
- Passing a test on Keeping Information Safe before we are allowed any access to the database
- Putting passcodes on our phones and tablets
- Using secure email or safe file sharing software when we need to share data electronically
- Scanning paper copies in to the database as soon as possible so that the

record is all kept in one place

- Using our company wifi when we are in the office and avoid using public wifi. If we are at home then we follow our policy on working from home
- Using approved IT equipment (such as encrypted laptops, mobile phones and computers) and approved software.
- Asking our IT to keep our systems' security up to date. For instance by updating the software and locking down our laptops so only approved memory sticks (USBs) can download information

## Have a secure attitude: Security thinking

### **We use our thinking to keep data safe by:**

- Never sharing passwords and changing them straight away if we think someone else might know them
- Using strong passwords that aren't easy to guess
- Using numbers (IDs) or initials to refer to people who use our service rather than full names
- Only looking at the records of the people we are working with, even if we have access to other records in the service
- Updating records within 48 hours
- Only keeping one copy of a record in the approved place
- Double checking details – spellings, contact details and numbers – before we use them (like checking the address on a letter before we post it)
- Telling our line managers (report an incident) if something has gone wrong. We then share what we've learnt with the people who work for us at team meetings or through our intranet
- Asking for help from our line managers or IG and IT security experts if we don't know what to do
- Making sure we have and knowing how to find an up to date plan so that we can still work if things go wrong (we call this a business continuity plan or BCP)
- Signing agreements with the organisations we share data with saying what we will share (the minimum needed to do the job), how we will share it and how we will protect the data (ISAs)
- Filling in Data Protection Impact Assessment (DPIA) before starting a new project that will affect people's data (our managers do this)
- Keeping track of any risks to information and data and putting steps in place to manage them

## → Resources: Keeping data secure

- [How to...Look after records](#)
- [How to...Assess the impact something will have on data protection \(complete a DPIA\)](#)
- [How to...Share information safely](#)
- [We Are With You National Business Continuity Plan \(BCP\)](#)
- Incident Management [Policy \(DQ199\)](#) and [SOP \(DQ199.1\)](#)
- [Case Management Policy and S.O.P. \(DQ163\)](#)
- Keeping Information Safe training ([Loop](#))
- [How to...Assess and manage risks to information](#)

### IT Policies:

- [IT Acceptable Use policy \(AUP\) \(DQ215 - ICTUP001\)](#)
- [Bring Your Own Device \(BYOD\) policy \(DQ216 - ICTUP002\)](#)
- [Electronic Communications policy \(DQ217 - ICTUP003\)](#)
- [Mobile Devices policy \(DQ218 - ICTUP004\)](#)
- [Mobile Phone Use policy \(DQ220 - ICTUP006\)](#)
- [User Passwords policy \(DQ221 - ICTUP008\)](#)
- [Wireless Access policy \(DQ222 - ICTUP009\)](#)
- [Working From Home policy \(DQ223 - ICTUP010\)](#)

If you need further help, email us at [support@wearewithyou.org.uk](mailto:support@wearewithyou.org.uk)

## Know what you need to do

Who	What they do
Everyone	<ul style="list-style-type: none"> <li>● Make sure the data you give or use is correct and up to date</li> <li>● Know your Information Rights – see our policy on the website</li> <li>● Read our privacy notices (the <a href="#">general privacy notice</a> on our <a href="#">website</a> and the ones at our services)</li> <li>● Ask questions if you have any</li> </ul>
People who work for us	<p>The same as Everyone (above), and:</p> <ul style="list-style-type: none"> <li>● Complete the Keeping Information Safe training every year</li> <li>● Read and follow our Information Governance policies (this one, Privacy, Sharing and Confidentiality and Information Rights) and our guidance (linked in policies)</li> <li>● Make sure the records you work with are kept safe, up to date and available only to those who need them</li> <li>● When something goes wrong, report the IG incident through the incident reporting software</li> </ul>
Managers	<ul style="list-style-type: none"> <li>● Make sure your teams have completed their training</li> <li>● Help resolve IG incidents and share learning</li> <li>● Check and sign off responses to requests for information (SARs) and record destruction</li> <li>● Keep track of the data in their service, the risks to it, how it's used and where it goes</li> <li>● Make sure the service's Information Sharing Agreements (ISAs) and privacy notices are up to date</li> <li>● Write Data Protection Impact Assessments (DPIAs) before introducing a new or changed project that will affect people's data</li> </ul>
Data Protection Officer: <a href="#">Jo Bevan</a>	<ul style="list-style-type: none"> <li>● Answers IG questions from people who work for us and people who use our services</li> <li>● Helps with tricky IG situations where the answer is not clear</li> <li>● Signs off agreements (ISAs) and assessments on our behalf</li> <li>● Knows all about data protection issues</li> <li>● Helps to resolve complaints and feedback</li> <li>● Reports serious IG incidents to the ICO</li> </ul>
Caldicott Guardian: <a href="#">Paul Hughes</a>	<ul style="list-style-type: none"> <li>● Knows all about the <a href="#">Caldicott principles</a></li> <li>● Helps when we are not sure whether to share information</li> </ul>

	about our service users in tricky situations
Information Governance Officer: <a href="#">Emma Bettany</a>	<ul style="list-style-type: none"> <li>• Answers IG questions and helps with tricky IG situations</li> <li>• Updates our policies, training and guidance</li> <li>• Keeps up to date on the current law and guidance</li> <li>• Helps services write their DPIAs, ISAs and privacy notices</li> <li>• Helps us show how important we think it is to look after records</li> </ul>
Information Security Officer: <a href="#">Stuart Horner</a>	<ul style="list-style-type: none"> <li>• Looks after IT related information security issues and risks</li> <li>• Helps us show how we keep records safe by getting safety certificates</li> <li>• Ensures our systems are up to date and tested</li> <li>• Reports to the IG Group</li> </ul>
Senior Information Risk Owner (SIRO): <a href="#">Company Secretary</a>	<ul style="list-style-type: none"> <li>• Is aware of all our information risk and the things we have in place to manage the risks</li> <li>• Ensures that everyone is aware of their personal responsibility to use good judgement, and to protect and share information safely</li> </ul>
Information Governance (IG) Group	<ul style="list-style-type: none"> <li>• Discusses IG across the whole organisation</li> <li>• Signs off our IG policies, training and guidance</li> <li>• Manages risks to information security and protection</li> <li>• Advises senior leadership</li> <li>• Helps us show how we look after records</li> </ul>
Chief Executive: Belinda Phipps (interim)	<ul style="list-style-type: none"> <li>• Has overall responsibility for how we look after records</li> </ul>



## Resources: Know your duty

- [Privacy, Sharing and Confidentiality policy](#)
- [Information Rights policy](#)
- Keeping Information Safe training ([Loop](#))
- [How to...Look after records](#)
- [How to...Understand the Caldicott principles](#)
- [How to...Assess and manage risks to information](#)

- [Ulysses incident reporting software](#)
- Incident Management [Policy \(DQ199\)](#) and [SOP \(DQ199.1\)](#)
- [How to...Assess the impact something will have on data protection \(complete a DPIA\)](#) - links to our DPIA template
- [How to...Share information safely](#)

If you need further help, email us at [support@wearewithyou.org.uk](mailto:support@wearewithyou.org.uk)

# Follow the Law

We think that it's important to look after people's data, and the law (GDPR 2016 and DPA 2018) says so too. There are plenty of [resources](#) to help us to take good care of data generally and as a health care organisation.

## Use the Data Protection Principles:

- [Lawfulness, Fairness and Transparency](#) – we tell people what we're doing with their data, that it's legal and not anything unfair or unexpected.
- [Purpose Limitation](#) – we only use data for what we've said we'll use it for
- [Data Minimisation](#) – we don't keep or share more than we need to do our jobs
- [Accuracy](#) – we make sure the data is up to date and right
- [Storage Limitation](#) – we only keep it for as long as we need to
- [Integrity and Confidentiality \(security\)](#) – we keep it safe and private
- [Accountability](#) – we take responsibility for the data in our care

## Use data fairly, clearly and in line with the law

We've written a policy about your Information Rights (available on our website) so you know exactly how you can access them with us. If you are a child (aged under 18 in England or under 16 in Scotland), the law says we must take special care with your data, and think about how to protect it when we are planning and running services.

## Data about service users

Under the GDPR, our "lawful basis" for using (processing) personal data is our "legitimate interests" as a healthcare charity. That means that we need the data so that we can work safely and well.

This includes "special category" data (things which are likely to be more sensitive) or criminal offence data, if we need it for your health care.

The types of special category data we collect about you include your race or ethnic origin, religious beliefs, information relating to your sexual orientation or sex life and health related information.

## Data about people who are working on our behalf

People who are working on our behalf may be:

- paid or unpaid employees

- agency workers
- contractors
- volunteers
- people who apply to work for us

For this data our lawful basis is “contractual”. That means we need your personal data so that we can employ and pay you as part of our contract of employment with you.

We only process “special category” data (things which are likely to be more sensitive) or criminal offence data, if we need it for your health care, or because the law says we must (called a “legal obligation”), or if it’s not essential but you say we can use it (“consent” is then our lawful basis).

The types of special category data we collect about you include your race or ethnic origin, religious beliefs, membership of a trade union, information relating to your sexual orientation and health related information.

## Be responsible for our data

In some of our services we may be the “data controller” (in charge of looking after the data), joint controllers with our partner(s), or a “data processor” (using data on behalf of the controller). We take good care of your data whatever our role, but we think it’s important to know what our role is so that we can best help you access your information rights.

When other people collect, use or store data for us, we make sure that they will also follow the law before we share any data. We tell them exactly what to do in an Information Sharing Agreement (ISA). Sometimes we ask people to sign a Non-Disclosure Agreement (NDA) which stops them telling others about the data we look after.

We’ve told the Information Commissioner’s Office (ICO) what data we will use and how we will use it (our registration number is Z7376908). We’ve also told them who our [Data Protection Officer](#) is. If we think something has gone wrong, we report it through our incident reporting software and then our IG experts take it to the ICO.

## Only use and share what we need to do our jobs

We use our guidance (like our Privacy, Sharing and Confidentiality policy), judgement and the information we have to decide whether or not to share. We try to understand why and how much information is needed and what question we are trying to answer. That way we can send as little data as possible. The less

data we send, the less there is that could get lost, stolen or misused. But we balance that against the danger of anyone working without all the facts.

## Know what data we have and where it goes

We update our information asset register every year. We use it to keep track of what information we have, where we keep it and where it goes (known as information flows). An “asset” is something that is valuable or important to us, and that’s how we feel about the data we hold. We make sure a senior member of staff is responsible for the asset (sometimes called an information asset owner).

### → Resources: Follow the law

- [Information Rights policy](#)
- [Privacy, Sharing and Confidentiality policy](#)
- [How to...Share information safely](#)
- [Data Protection Act \(DPA\) 2018](#)
- [General Data Protection Regulation \(GDPR\) 2016](#)
- [Information Commissioner’s Office \(ICO\) website](#)
- [Children and the GDPR \(ICO guide\)](#)
- [Ulysses incident reporting software](#)
- Incident Management [Policy \(DQ199\)](#) and [SOP \(DQ199.1\)](#)
- [How to...Assess and manage risks to information](#) (assets)

If you need further help, email us at [support@wearewithyou.org.uk](mailto:support@wearewithyou.org.uk)

Policy version history	
Policy Title	Data Security and Protection Policy
Policy Number	DQ402
Version Number	1

Date of Issue	Sept 2020
Date of Review	Sept 2021
Sponsor	Deputy CEO

Issue	Page(s)	Issue Date	Additions/Alterations
1	17	Sept 2020	New policy simplifying and replacing existing IG policies.