

[View this email in your browser](#)

www.onewest.co.uk



Spare a thought

28th January was **World Privacy Day**. The aim of this annual event was to help spread understanding of **rights and responsibilities when handling data**.

It's hoped that the day will help create a legacy of **understanding** and **behaviours** to help protect all of us going forward.

The **relevance** of this in an ever increasing data controlled world is huge – it touches on all our lives and we need to make sure that our children grow up safely in this changing environment. This need is there all year round not just on the day itself.

There is a strong **legislative framework** in place via **GDPR** and the **ICO** is showing it has teeth handing out some significant fines to some organisations already.

The **potential** in organisations for data breaches is huge and in truth many find the prospect of a breach scary and want to make every effort to reduce the risk of one.

The good thing is that with **effective support** it is all doable – however there are some really important things to know.

So what if a data breach happens?

Most data breaches relate to information being sent to the wrong address and, in most cases it is possible to contain these incidents.

However, breaches occasionally require more action to avoid harm coming to an individual, and in some cases police involvement may be required.

Rapid identification and a coherent report are critical to allowing your organisation to contain, recover and report data breaches as required to by law. Employees need to follow some simple steps to ensure that data breaches, incidents and near misses are managed effectively:

1. Identify

A breach can be the loss, destruction, inadvertent disclosure or inappropriate access to data.

2. Contain

Can you restore, recover or deny access to data to avoid any escalation of the breach?

3. Report

If you work with us use the Incident Reporting Form on the One West website (or request a copy via email) and send it to i-west@bathnes.gov.uk. When in doubt, always report.

4. Support

Where necessary companies like One West will provide guidance on follow up steps, including containment, reporting the incident to the ICO, and communicating the breach to the data subject.

What can help lower the risk of a breach?

Many incidents can be avoided with adequate **training, awareness** and **guidance**

There are some good areas of best practice

1. Always lock your screen when leaving your desk.
2. Be aware of your surroundings when working in a shared space - should you take this conversation in a private room?
3. Set a delay on your emails - if you quickly spot a mistake (e.g. wrong recipient, or wrong attachment) you can fix it before it is sent.
4. Always clear a paper jam (or delete your job) before leaving a printer - there could be personal data jammed in the machine, that someone else could get hold of.
5. Keep a clear desk - put away any personal data into a drawer or cupboard where possible at the end of the day.

Effective treatment of confidential waste is essential

Within your organisation there should be a system in place to ensure that all records containing personal data are disposed of confidentially. There are several options to do this, for example information may be shredded on site, or disposed of in sacks to be collected by a confidential waste company (which should be adequately secured when stored for collection). When personal data which is not disposed of correctly, it counts as a data breach.

Many people aren't sure what they should be disposing of confidentially, and what they can just put in the bin. Your confidential waste includes:

Any record which details personal information

This includes:

- anything which relates to and identifies a living person, or could help someone identify a person when used with other information
- is an expression of opinion about an individual
- indicates our intentions towards an individual

E.g. Name, Address, Date of Birth, Email, Phone numbers, Location data, IP addresses

Any record which details sensitive personal information

This includes:

- Race and/or ethnicity
- Political opinions
- Religious beliefs (or other beliefs of a similar nature)
- Trade Union membership
- Biometric or physiological information e.g. Photos
- Mental or physical health condition
- Sexual life and orientation
- Criminal records (actual or suspected)

E.g. Safeguarding, Accident/First Aid, Equalities information, Legal records

Any record which details business / commercially sensitive information

This includes information which your organisation would be affected by any loss of, or unauthorised access to.

E.g. Contracts, opinions on service delivery, tender information.

It is also important to understand that a record can be in almost any format – e.g. Paper, Post-it notes, Disks, CDs, Tapes, Posters etc. Make sure you have an appropriate method of confidentially destroying non-paper records. **If you have any doubt – treat the information as confidential.**



Copyright © 2020 One West, All rights reserved.

Our mailing address is:

One_West@bathnes.gov.uk

Want to change how you receive these emails? Just let us know
