



# HIDDEN DATA

Sharing data is vital for organisations to operate but data loss is a significant issue which can have a severe impact on those involved. One easy way to prevent the accidental publication of data not intended for release is to check spreadsheets, charts and tables for hidden data before sharing them.

## Four common types of hidden data

### 1 Data hidden in plain sight

This means that data could be hidden when the text is the same colour as the background (e.g. white text on a white page). This data can be exposed by highlighting the text or changing its colour.

### 2 Hidden rows and columns

It is common for rows and columns to be hidden in Excel and they can usually be spotted where the numbers and the letters in the headings are not running consecutively. You could also use the Document Inspector by clicking on File>Info>Check for Issues>Inspect Document.

### 3 Hidden sheets

Entire sheets of data can also be hidden, and they can be harder to spot. The easiest way to check for hidden sheets is to right click on any sheet tab and see if the "Unhide" option is enabled. You could also use the Document Inspector by clicking on File>Info>Check for Issues>Inspect Document.

### 4 Pivot tables and charts

Underlying source data is not always visible in pivot tables and charts, but it can still be extracted. Exporting or saving spreadsheets into a simple text format such as CSV is a good way of ensuring all hidden data can be inspected prior to sending.

### What if I share hidden data by mistake?

By following the information contained within this document we can reduce the number of incidents of accidental data loss across government. However, we understand accidents can happen. If you realise you have accidentally shared hidden data don't panic but do take prompt action:

- If the information was sent by email, try to recall the email as soon as possible.
- If you can't recall it, contact the person who received it and ask them to delete it.
- As soon as you spot the mistake, contact your line manager or local security team.

It is important you understand your local reporting procedures because reporting incidents early can prevent harm.

**SOME THINGS  
YOU CAN'T UNDO**