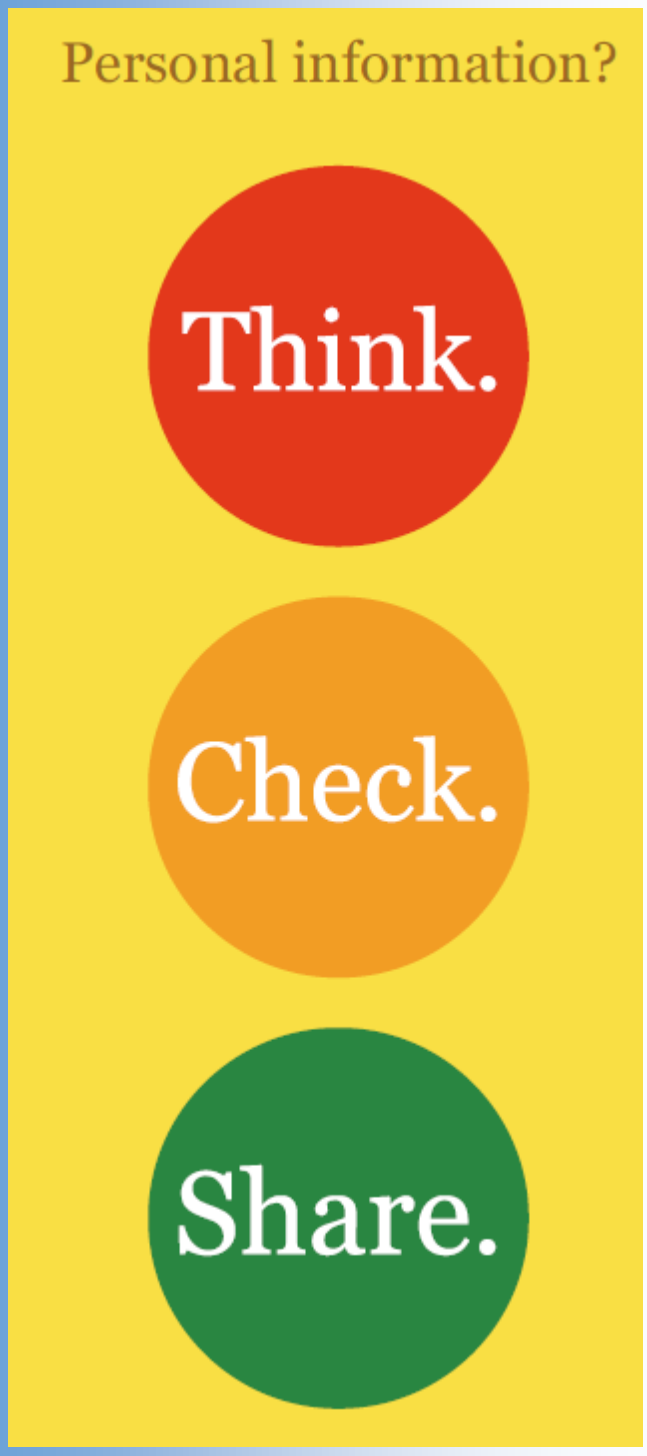


Data Protection Awareness & Procedures (Including GDPR)

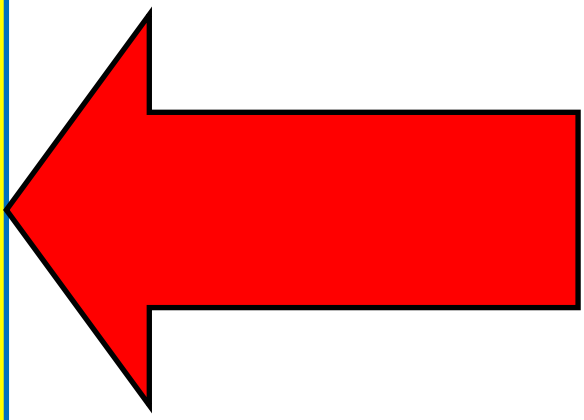
Glossary: The jargon explained:

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt-in basis rather than opt-out.

Data controller is the person or organisation who determines the how and what or data processing.

Data subject is the persona about whom personal data is processed.

Personal data is information about a living individual which is capable of identifying that individual. E.g. a name, email address, photos.



Privacy notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing).

Sensitive personal data is also described as 'special categories of data'—see individual page on this category.

Source: NALC

The General Data Protection Regulation (GDPR) and Data Protection Act 2018

What changed?

- Greater clarity over the use of personal data
- Proof of consent* required for data sharing
- Enhanced rights of access for data subjects
- Mandatory data breach disclosure within 72 hours to the ICO

Saltash Town Councillors

Saltash Town Councillors (and prospective Councillors) are no longer required to be registered as Data Controllers following an amendment to the Data Protection Regulations from 1st April 2019. Members previously registered will have their details removed by the ICO in due course.

However, this change to legislation does not remove the responsibility that all members have to continue to operate within the boundaries of the regulations.

CHILDREN

Children have the same rights as adults over their personal data but only those above the age of 13 can give their consent if this is the lawful basis being relied upon. Below that age consent has to be from someone with parental responsibility and reasonable steps should be taken to confirm their identity. Safeguarding should also be a consideration.

Before processing data from children please seek additional advice.

PERSONAL INFORMATION

Personal Information is:

Name

Address

Phone Number

Email Address

IP Address

Cookie Records

It can also be information that someone could identify a person from within correspondence.

Personal information for the purpose the data protection is that of a living individual.

Personnel Information and records

It does not include:

Councilors' contact details as they are public officers

Business contact details and correspondence

Charity or Community Group officer/secretary contact details and correspondence

The deceased

It does include :

Parishioners and members of the public:

Contact details

Hard copy correspondence

Email correspondence

Complaints

Consultation forms

Personal data should 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 central to GDPR. Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

ico.
Information Commissioner's Office

We're getting ready for GDPR. Are you?

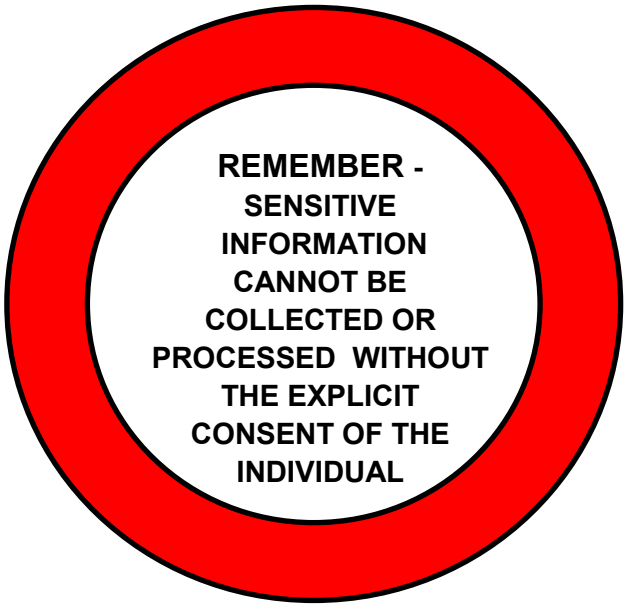
The GDPR provides the following rights for individuals:

The right to be informed	Individuals need to know that their data is collected, why it is processed and who it is shared with.
The right of access (Subject Access Requests)	Individuals have the right to access their personal data.
The right to rectification	Personal data should be accurate and up to date
The right to erasure	Individuals have the right to be forgotten and can request the erasure of their personal data.
The right to restrict processing	Individuals have the right to block or restrict the processing of personal data.
The right to data portability	Individuals can obtain and reuse their personal data for their own purposes across different services.
The right to object	Individuals must be advised of their right to opt out of processing activities.
Rights in relation to automated decision making and profiling	The right not to be subject to a decision based solely on "automated processing " including profiling.

INDIVIDUAL RIGHTS

Sensitive Data
(also known as Special Category)

Under the GDPR and Data Protection Act 2018 this type of data requires more protection.



You must determine and record the lawful basis for processing this type of data before beginning.

A Data Protection Impact Assessment will be necessary.

Types of special category data:

- Race;
- Ethnic Origin;
- Politics;
- Religion;
- Trade union membership;
- Genetics;
- Biometrics (where used for ID purposes);
- Health;
- Sex life;
- Sexual orientation.

Information relating to criminal convictions has to be handled in a different manner. If you need to process this type of data seek advice from the ICO.

SENSITIVE DATA: CARE

Data sharing checklists

These two checklists provide a handy step by step guide through the process of deciding whether to share personal data. One is for systematic data sharing, the other is for one off requests.

The checklists are designed to be used alongside the full code and highlight the relevant considerations to ensure that the sharing complies with the law and meets individuals' expectations.

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis

Is the sharing justified?
Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

ico.
Information Commissioner's Office

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances

Is the sharing justified?
Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?
Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share
Key points to consider:

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate/safe to inform the individual that you have shared their information.

Record your decision
Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

SECURITY

SECURITY

RISK MINIMISATION IS ESSENTIAL

Computers & Paperwork:

- **All computers should be password protected (and the password regularly changed).**
- **If you leave your workstation ensure the computer is locked and no paperwork with personal information is left in public view.**
- **Filing cabinets should be locked.**
- **Dispose of all waste paper appropriately.**

In public areas:

- **Be aware when discussing personal data—a breach can be verbal.**
- **Ensure no paperwork or computer monitors with personal data are visible to members of the public.**

Outdoor working (eg Meet your Councillors):

- **Mobile devices should be pin protected and never left unattended.**
- **USB sticks should be encrypted and password protected. It is good practice to ensure no personal data is held on a portable media device.**
- **Laptops should be password protected, never left unattended in public places and not hold any personal data on the local hard drive.**
- **Paperwork with personal data, and in particular sensitive personal data should be handled with extreme care.**

Emails:

Most security breaches happen because of distractions or mistakes. Check email addresses and contents before clicking send!

Reply to all is not advisable—you do not know who might be Bcc'd into the email you are replying to.

Data Breaches

DATA BREACHES

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberation causes. It also means that a breach is more than just about losing personal data.

Example:

Personal data breaches can include:

- Access by an authorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect person;
- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission;
- Loss of availability of personal data.

(Source: ICO Guide)

Personal data breach = a security incident affecting confidentiality, integrity or availability of personal data

If you become aware of a data breach contact the Senior Policy & Data Compliance Monitoring Officer for advice.

YOU ARE REQUIRED TO REPORT ANY DATA BREACHES WITHIN 72 HOURS.

The ICO website is constantly updating their resources on Data Protection and GDPR. You can register to receive updates by email. The website is a good source of information and the enquiry line is also there to help with any queries you may have.

Website: www.ico.org.uk