How we handle your data safely and securely

*All data held by ADR Scotland follows the '*__five safes framework__*' - a set of principles devised by the Office for National Statistics that ensure the secure and effective access and use of data, alongside relevant legal basis and gateways.*

1. Safe Projects; research that is legal, feasible and ethical

- Research projects using ADR Scotland data must be approved by an appropriate body and be in the public interest.

2. Safe People; researchers can be trusted to work safely with data

- Researchers or anyone wishing to access data held by ADR Scotland must complete relevant training – which can be chosen by the data controller.

3. Safe Setting; appropriate secure environments to prevent misuse

- Those accessing data must access it within the National Safe Haven, located within the University of Edinburgh. This secure infrastructure recently received DEA (Digital Economy Act) accreditation and has multiple controls to prevent misuse and support sensible use of data.

4. Safe Data; sufficient detail but without excessive risk

- The ADR Scotland infrastructure minimises the amount of data that is accessible to any party at a time. Datasets created for approved research projects from datasets held by ADR Scotland use the minimal amount of data needed for that project.
- A single organisation will never have all the information about a complete dataset or an individual which further minimises any potential risk.

5. Safe Outputs; safeguards in place ensure the confidentiality of data subjects

- All information leaving the Safe Haven (such an analysis tables or other research outputs) undergo strict disclosure control by the electronic Data Research and Innovation Service (eDRIS). This may involve changing outputs so that the findings remain clear but are less likely to identify individuals or small groups.

Underpinned by legal basis and gateway

- ADR Scotland will always ensure that data is shared using an appropriate legal basis and gateway to fully comply with data protection legislation and offer data controllers support completing relevant documentation to demonstrate compliance.