# DRAFT RCS Data Breach policy and procedure.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. Where feasible, this must be done within 72 hours of becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, those individuals will be informed without undue delay.

RCS will ensure it has robust breach detection, investigation and internal reporting procedures in place. This will help facilitate any decision about whether or not we need to notify a relevant supervisory authority and the affected individuals.

RCS will keep a record of any personal data breaches, regardless of whether we are required to notify.

### **What is a personal data breach?**

A personal data breach is 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 deliberate causes.

Personal data breaches could include:

* Access of personal data by an unauthorised party
* Deliberate or accidental action or inaction by a controller or processor.
* Sending personal data to an incorrect recipient
* Computers being lost or stolen
* Alteration of personal data without permission
* Loss of availability of personal data

**Responsibilities in the event of a personal data breach incident.**

RCS should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

Where RCS is not the data controller, we must inform the data controller without delay.

Where RCS is the data controller, we must also tell the data subject and the Information Commissioner’s Office (ICO) if required.

**Who in RCS must be told (the supervisory authority)?**

A data breach of any size is a crisis management situation and a breach response will involve people in a number of roles.

It should be reported to (or by) the organiser in the first instance and to the Data Protection Officer and to the Trustees via the line manager.

**What information about a breach must we provide to individuals.**

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. This should take place as soon as possible particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. RCS will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

**What information we must give the ICO about a breach.**

The ICO will ask questions about:

* What has happened.
* When and how you found out about the breach.
* The people that have been or may be affected by the breach.
* What you are doing as a result of the breach.
* Who we should contact if we need more information and who else you have told.

**RCS Personal Data Breach response procedure**

* Ensure physical security of premises if required.
* Secure and isolate any potentially compromised devices and data, without destroying evidence.
* Pause any document destruction processes.
* Report the personal data breach to the RCS supervisory authority.
* Gather information about the breach includinf taking statements from staff and volunteers who may have information to contribute.
* Log the steps taken in the investigation.
* Document the breach.
* Assess the likely risk to individuals of the breach.
* Establish what external expertise may be needed.
* Inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms without undue delay.
* Where RCS is not the data controller, notify the data controller.
* Notify insurers.
* Notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

**Important:** confidentiality must be maintained throughout the breach investigation and reporting processes.

**Information Commissioners Office**

The ICO personal data breach helpline can offer advice about what to do after experiencing a personal data breach, including how to contain it and how stop it happening again. They can also offer advice about whether we need to tell the data subjects involved.

To report a breach, call the ICO helpline on 0303 123 1113.