Data Breach policy

Reviewed and adopted November 2020
Next review due November 2022

Policy Statement

This policy accompanies our Data Protection and Privacy policy to set out the process should there be data breach. Read for Good collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Purpose and Scope

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents and relates to all personal data held by Read for Good regardless of format.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definitions / Types of breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to Read for Good's information assets and / or reputation.

An incident includes, but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record)
- Equipment theft or failure
- System failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data
- Website defacement
- Hacking attack

- Unforeseen circumstances such as a fire or flood;
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

Any individual who accesses, uses or manages Read for Good's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO).

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (see form at end).

All staff should be aware that any breach of Data Protection legislation may result in Read for Good's Disciplinary Procedures being instigated.

Containment and recovery

The DPO will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant people to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause. The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate. The LIO, in liaison with the relevant people will determine the suitable course of action to be taken to ensure a resolution to the incident.

Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur. The investigation will need to take into account the following:

- The type of data involved
- Its sensitivity
- What protections are in place (e.g. encryptions)
- What has happened to the data (e.g. has it been lost or stolen)
- Whether the data could be put to any illegal or inappropriate use
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

Notification

The LIO in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation
- Whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Whether there are any legal / contractual notification requirements
- The dangers of over notifying: not every incident warrants notification and over notification may cause disproportionate enquiries and work

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay.

Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Read for Good for further information or to ask questions on what has occurred.

The LIO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

The LIO will discuss with the wider team consider whether a press release is required and prepare to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the LIO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie including identifying potential weak points within existing security measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Staff awareness

- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Board of Trustees.

Read for Good Policies in Practice

- This policy is reviewed on the date shown by the CEO, Operations Manager (and DPO if different), with any changes approved by the Board of Trustees.
- Overall responsibility for this policy and its implementation lies with the Board of Trustees delegated to the CEO.
- This policy applies to all Read for Good personnel (including staff, trustees, and volunteers) because data is crucial to how we run our charity and all roles within the organisation have access to, and process this data. Trust in our data and privacy process is fundamental.
- This policy is shared with all relevant personnel via: induction, team meetings, board reports, website, shared drive.
- Read for Good ensures implementation and compliance of this policy by: making sure staff have appropriate input into the review process, discussion and training, leadership team modelling and reinforcing policy content into day to day work, by trustees showing focus and leadership over policy issues and a regular review process.
- Any service user who believes that this policy is not being followed should refer to Read for Good's Complaints policy. Internal complaints or concerns about adherence to the policy are handled with regular opportunities for all staff to speak in confidence to their manager, or the CEO or Trustee if the complaint or concern is about their line manager or CEO not adhering to a policy. Staff are encouraged to explain clearly what the lack of adherence relates to. The CEO and the person responsible for the policy have the opportunity to discuss the issue, and establish if it is a systems error, or an individual issue. For a systems error, systems will be improved and updated, and training for all staff will be undertaken. In a case of clear policy breach by an individual, the individual is given an opportunity to correct their error. If the adherence issue is persistent then training and monitoring will be offered and implemented, with reviews at appropriate points. Continued breaches may put the individual at risk of dismissal.

Data Security Breach Reporting Form

Section 1: Notification of Data Security Breach: To be completed by person reporting the incident	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the DPO	
Received by:	
On (date):	
Forwarded for action to:	
On (date):	
Name of person investigating breach (LIO) Name Job Title Email Phone number	
Section 2: Assessment of Severity: To be completed by the Lead Investigation Officer in consultation with the Head of area affected by the breach and if appropriate IT	
Details of information loss:	
How many data subjects are affected?	
What are the potential consequences on the individuals affected? - Are there any measures they can take to safeguard against the breach; - Are there any costs to taking those measures?	
Assessment of ongoing risk	
Have the affected individuals been contacted? Individuals contacted (list or link) Method of contact used to contact? What was said?	
Details of the IT systems, equipment, devices, records involved in the security breach	
If laptop lost/stolen: how recently was the laptop backed up onto central systems?	

Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for us or others?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories: **HIGH RISK personal data** • Special categories of personal data (as defined in the Data Protection Legislation) relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions or religious beliefs; c) trade union membership; d) genetics; e) biometrics (where used for ID purposes) f) health; g) sex life or sexual orientation • Information that could be used to commit identity fraud such as:personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; Personal information relating to vulnerable adults and children; • Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Security information that would compromise the safety of individuals if disclosed.	
Section 3: Action taken: To be completed by DPO and/or Lead Investigation Officer	
Incident number	e.g. year/001
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Was incident reported to Police? Time and method of contact Name of person contacted Contact details Next steps	Yes/No
Follow up action required/recommended:	
For use of DPO and/or Lead Officer:	
Notification to ICO https://report.ico.org.uk/security-breach/ If YES, notified on:	YES/NO
Notification to data subjects If YES, notified on:	YES/NO
Notification to other external, regulator/stakeholder If YES, notified on:	YES/NO