SCHR[1] MISCONDUCT DISCLOSURE SCHEME - Data Protection Impact Assessment

Date of next review: 3 years from sign-off

[1] The Steering Committee for Humanitarian Response: https://www.schr.info/

Contents

Table of Contents

Table of Contents 2
Change Log 3

Project Overview 4
Submitting controller details 4
Key Project Stakeholders & Roles 4

Summary of the Scheme and its Purpose 5

Information flows 7
Collection, use and deletion of data 7

Compliance with Data Protection Principles 10
Transparency 10
Legality 10
Security 10
Data adequacy and data minimisation 12
Rights of the data subject 13

Risk Assessment 14
Risk log and Mitigation plans 14
Information Commissioner's Office (ICO) Consultation 18

Conclusion 19
Conclusion 19
Review schedule 20
Sign-off 21

Appendices 22
Appendix 1 – Supporting documentation – Questionnaires 22
Supporting documentation – Statement of Conduct Template 23

Glossary & Acronyms 24

Version control

Change Log			
Version	**Date**	**Initials**	**Description of change**
0.1			

Project Overview

Data Controller details

Name of controller	British Red Cross Society
Subject/title of DPO	Data Protection Officer
Name of DPO	Milgo Ali

Key Project Stakeholders & Roles

Key Stakeholders		
Name	**Role**	**Project role**
Gaelle Pertot	International HR Project Adviser	Project Adviser
Steph Harris	Head of International HR	Authorised HR
Rebecca Curtis	Advice and Casework Manager	Authorised HR
Maureen Kerrigan	People Support Manager	Authorised HR

Data processing responsibilities	
Name	**Role**
International HR and People Support	Requesting and receiving Statement of Conduct
International HR Advisers + HR Advice and casework + People Support	Completing Statement of Conduct
British Red Cross Society	Data Controller & Data Processor
Individual applying for a job at the British Red Cross Society	Data Subject
British Red Cross Society staff member	Data Subject
Applicant's previous employer	Data Controller & Data Processor
Organisations participating in the Scheme	Data Controller & Data Processor

Summary of the Scheme and its Purpose

Purpose of the Scheme

The purpose of the SCHR Misconduct Disclosure Scheme (the Scheme) is to establish a minimum standard for humanitarian, development and other civil society organisations to share information as part of their recruitment process about people who have been found to have committed sexual harassment, sexual abuse or sexual exploitation (collectively defined in this document as "**Misconduct**") during employment. It complements the work that organisations are already doing as part of their recruitment processes.

The Scheme ensures that all organisations who sign up to it work to a common minimum exchange of relevant sensitive information, while respecting applicable legal and regulatory requirements. See below for more information:
https://www.schr.info/the-misconduct-disclosure-scheme

The three commitments that the BRC is signing up to are:

- To systematically check with previous employers about any findings of Misconduct against potential new hires;
- To respond systematically to such checks from others; and
- To monitor certain data and submit it to SCHR on a regular basis - more information here: https://www.schr.info/implementation-data

The Scheme is currently implemented by multiple organisations: https://www.schr.info/mds-registry ("**Participating Organisations**")

Benefits to the BRC and others

Participation in the Scheme will benefit the BRC, the Participating Organisations, the public, and individuals served by the aid sector by:

- Identifying potential new hires who may have a history of Misconduct in the aid sector.

- Sharing information on a systematic basis with the aim of preventing such individuals from working at another aid organisation, where appropriate.
- Protecting the vulnerable individuals the sector serves.
- Preserving trust in the aid sector and the organisations who participate in it (which is in turn likely to have an effect on donations made to the sector).

Identification of the need for a DPIA

In general terms, the need for a DPIA was originally considered due to the investigation constituting a major project involving the use of Personal Data. In such circumstances it is important for the BRC to ensure that a process is carried out to identify and minimise the data protection risks.

It was decided that a DPIA should be conducted in the context of the Scheme for the following reasons:

- The processing may prevent data subjects from securing a job in the aid sector.
- The Scheme may involve processing of sensitive data, data of a highly personal nature or criminal-offence data.
- The Scheme involves processing personal data on a large scale.

Information flows

Collection, use and deletion of data

Participating Organisations will share Misconduct History relating to data subjects who work, or have in the past worked, for the Participating Organisation as an employee with other Participating Organisations.

When a Participating Organisation is recruiting a candidate (a "**Recruiting Organisation**"), they will request personal data from the organisation in which the candidate works or worked within the previous five years as part of their recruitment process (i.e. the process by which each Participating Organisation assesses the suitability of an individual for a position);

A Participating Organisation who is contacted by a Recruiting Organisation (a "**Responding Organisation**") will complete a Statement of Conduct upon request to respond to a request for information. A suggested template Statement of Conduct is provided to Participating Organisations

The Recruiting Organisation will use information contained in Statement of Conduct to inform the decision as to whether to hire or appoint the data subject.

Types of Personal Data likely to be captured include:

- Full name
- Dates of employment
- Whether the candidate was found to have committed Misconduct during the period of employment with the Responding Organisation
- The nature of the Misconduct
- The Disciplinary Measure imposed for the Misconduct
- The date of the Disciplinary Measure by the Responding Organisation
- Confirmation as to whether the candidate is currently being investigated for an allegation of Misconduct.

Special category data is also likely to be collected, including sexual orientation data. Criminal offence data is also likely to be collected.

What	Requesting a statement of conduct for new candidate	Receiving a statement of conduct request for previous/current staff
When	During onboarding process – prior to contract issued.	When another participating organisation is recruiting staff that have been previously working for BRC
Why	Reduces the hiring of individuals where allegations of SEA have been substantiated and also get information regarding unsubstantiated allegations, if someone leaves during an investigation.	Help the external organisation to reduce the hiring of individuals where allegations of SEA have been substantiated and to enable BRC to identify individuals who committed Misconduct during previous employment, or were under investigation for Misconduct at the time of their resignation, enabling BRC to judge their

		suitability for employment with us.
For whom	All new roles of International Directorate including UK-based, Overseas, and IFRC/ICRC seconded delegates.	When a leaver joins a new participating organisation, the employer will request a statement of conduct from us as part of their recruitment process
How	Statement of conduct process incorporated in our referencing request onboarding process.	Statement of conduct to be completed and forwarded to participating organisation ;

Storage of data

Data of completed statements of conduct will be kept on files as per references for staff. An access control system applicable to all users accessing the files is implemented. When granting access or assigning user roles, the "principle of least privilege" is observed in order to limit the number of users having access to the files only to those who require it for achieving the processing purposes.

Retention and deletion

- BRC employees: Year in which employee leaves BRC plus 6 further years
- 12 months for unsuccessful candidates. This is to ensure correct annual reporting to the MDS and is in line with retention period for external candidates.

Personal data will be deleted after the above timeframes have expired.

The nature and purpose of the Scheme means that it is anticipated that Misconduct History will be shared with registered Participant Organisations and Authorised Personnel within such organisations which is maintained by the SCHR.

Individuals affected

The Scheme will affect all candidates who apply for roles at Participating Organisations.

In addition, it will affect to some extent the internal stakeholders authorised to complete the Statement of Conduct, share it with others, and make decisions based on the receipt of a Statement of Conduct from a Participating Organisation.

Context of the processing

The relationship between the Participating Organisation and the data subject shall be that of:

- Employer and employee;
- Organisation and member of the organisation's governing body (for example, trustee or non-executive director); or
- Organisation and applicant for employment or office.

No children's data will be processed under the Scheme and it is not anticipated that personal data of other vulnerable groups will be processed.

The Scheme is a novel arrangement and is intended to be consistent with, and support implementation of, the Core Humanitarian Standards on Quality and Accountability (CHS). It is also designed to support international, national and local safeguarding measures and schemes.

The processing is of substantial public interest to respond to a recognised problem of repeat Misconduct in the aid sector and to protect the vulnerable individuals the sector serves. The processing represents a variation of existing referencing processes which are within data subject expectations and are widely accepted publicly as a legitimate means to protect organisations, their staff, and those they work for.

We are not aware of any specific prior concerns around referencing processes and, indeed, data subject access rights in relation to confidential references for employment have been reduced in the UK under the GDPR which appears to reflect the significant societal and organisational benefits of candid disclosures between employers on material matters. In this respect, data subject transparency around Statements of Conduct under the Scheme exceeds regulatory requirements

This DPIA covers: (i) the processing activities of sharing data in a Statement of Conduct between Participating Organisations; (ii) the processing activities which produces the Statement of Conduct; (iii) internal storage, retention and destruction.

Consultation requirements

Data subjects have not been consulted specifically in relation to this Scheme, since this would involve consulting with all employees and office-holders across the Participating Organisations externally, which would be disproportionate. However, the BRC has carefully considered the privacy risks associated with the investigation in order to ensure that these are addressed. However, staff have been informed and consulted during the launch of the process.

In addition, external employment lawyers and safeguarding experts have been consulted, as have internal stakeholders.

Compliance with Data Protection Principles

Transparency

Communication:

- Existing employees - BRC will communicate the Scheme process by email to all International Directorate Staff, and will update relevant policies accordingly, including the Employee Privacy Notice. The HR Project Adviser will be a contact point for answering any questions. If an investigation is required or a staff member faces a formal warning for Misconduct, the BRC will inform the data subject about our involvement in the Scheme.
- Potential new hires - The individual will be informed during the application process that obtaining the Statement(s) of Conduct is a mandatory part of our recruitment process for International Directorate Staff.

Legality

Data processing carried out for the purposes of participating in the Scheme will be based on grounds of legitimate interest, plus (if the personal data constitutes special category data) public interests.

The legitimate interests of the BRC (and other Participating Organisations) are to ensure that they only recruit candidates who can safely work with the communities and individuals they serve. Subject to the risk-mitigation measures outlined in this assessment, the BRC believe these interests are not overridden by the interests and rights of those whose data will be processed under the Scheme. The BRC has prepared a Legitimate Interests Assessment (LIA) in relation to the Scheme, which can be found at Appendix 1 – Supporting documentation.

Any data shared which contains details of an individual's sex life and/or sexual orientation (or enough information that someone could infer such details) will constitute special category personal data. To process special category personal data, BRC relies on the **substantial public interest** condition in Article 9(2)(g) GDPR), specifically that the processing is necessary for: (1) **preventing or detecting unlawful acts** (paragraph 10, Part 2, Schedule 1, Data Protection Act 2018) and/or (2) **Protecting the public against dishonesty** (paragraph 11, Part 2, Schedule 1, Data Protection Act 2018; and/or (3) **regulatory requirements relating to unlawful acts and dishonesty** (paragraph 12, Part 2, Schedule 1, Data Protection Act 2018) and/or (4) **safeguarding of children and of individuals at risk** (paragraph 18, Part 2, Schedule 1).

Any potential criminal offence data under Article 10 of the GDPR will be processed under the same conditions as above (per Section 36, Part 3, Schedule 1 of the Data Protection Act 2018.

Security

The Statement of Conduct form will only include official conclusions of reports and disciplinary processes (unless there are exceptional circumstances). The Scheme has

produced a template Statement of Conduct form with limited data fields to facilitate data minimisation.

Statements of Conduct forms are only created and shared by Authorised HR Personnel within a Participating Organisation on a need to know basis. Within BRC, internal security measures will be managed by International HR and HR Advice and Casework. An access control system applicable to all users accessing the IT system is implemented. The system allows creating, approving, reviewing and deleting user accounts. When granting access or assigning user roles, the “principle of least privilege” is observed in order to limit the number of users having access to personal data only to those who require it for achieving the processing purposes. Where authentication mechanisms are based on passwords, BRC requires the password to be at least eight characters long and conform to very strong password control parameters including length, character complexity, and non-repeatability. The authentication credentials (such as user ID and password) is never transmitted unprotected over the network. Data can only be accessed through 2 factor authentication where statements are stored on staff files.

Misconduct Histories will only be shared with, and accessed by, Authorised HR Personnel within BRC. An up-to-date list of Organisations and Authorised Personnel will be maintained by the Scheme: https://www.schr.info/mds-registry

Personal data will be shared under the Scheme using agreed secure methods, including: Email encryption and password protection of files.

Data adequacy and data minimisation

The personal data collected through the operation of the scheme is believed to be adequate, relevant and limited only to the personal data which is necessary to achieve the aims of the Scheme.

Data Minimisation		
Form	**Data item name**	**Justification for capture/ storage**
Statement of Conduct	Applicant full name	To help identify the individual who is applying for the role and enable the successful completion of the Misconduct background check
Statement of Conduct	Current staff/leaver full name	To help identify the individual who is applying for the role and enable the successful completion of the Misconduct background check
Statement of Conduct	Dates of employment	To help identify the individual who is applying for the role and enable the successful completion of the Misconduct background check
Statement of Conduct	Whether the candidate was found to have committed Misconduct during the period of employment with the Responding Organisation	To enable the successful completion of the Misconduct background check
Statement of Conduct	The nature of the Misconduct	To enable the successful completion of the Misconduct background check
Statement of Conduct	The Disciplinary Measure imposed for the Misconduct	To enable the successful completion of the Misconduct background check
Statement of Conduct	The date of the Disciplinary Measure by a Participating Organisation	To enable the successful completion of the Misconduct background check
Statement of Conduct	Is the Candidate currently being investigated for an allegation of Misconduct	To enable the successful completion of the Misconduct background check

Rights of the data subject

The BRC will respect and uphold data subject rights and data subjects will be informed that all such requests can be directed to the Information Governance team at dataprotection@redcross.org.uk. These rights are:

- Right of access - Subject Access Request (SAR)
- Right to Erasure of personal data concerning them
- Right to rectification of inaccurate or incomplete personal data concerning them
- Right to restriction of processing (in certain circumstances)
- Right to data portability
- Right to object and rights relating to automated decision-making (in certain circumstances) although the Scheme will not involve automated decision making.

Risk Assessment

Risk log and Mitigation plans

Risk refers to the combined likelihood the event will occur and the impact on the data processing if it does occur. The log includes a description of each risk, analysis and a plan to manage it.
Both likelihood and impact should be scored either 1, 2 or 3 – 1 being the lowest, 3 the highest. Each scoring level has the following logic underpinning it:

	Risk scoring	
	Likelihood (assuming no mitigation)	**Impact** (assuming no mitigation)
1	• Not at all likely	• No effect on data subject
2	• Might happen	• The data subject could experience some negative effects
3	• Will almost certainly happen	• The data subject would almost certainly be negatively impacted

Severity
Risk severity 'levels' are scored in the following way:

- 1-3 – Low risk – Green
- 4-6 – Medium risk – Amber
- 7-9 – High Risk – Red

These risk scores are in the severity column and are calculated in the following way:
*(**Likelihood** of risk happening x the **impact** on the processing)*

The risk log assesses two distinct types of risk:

- Inherent Risk
    - The risk **before any mitigation steps have been accounted for**, e.g. *the likelihood of a beekeeper being stung by a bee is very high, with medium impact*
- Residual Risk
    - The risk **after the mitigation steps have been implemented** and are active, e.g. *mitigation: beekeeper wears a protective suit; the likelihood of a sting is very low, with medium impact*

BritishRedCross

Risk log								
Risk log								
	Inherent Risk				**Residual Risk**			
Risk description	**Likelihood**	**Impact**	**Severity**	**Mitigation Plan**	**Likelihood**	**Impact**	**Severity**	**Owner**
Data subjects are prevented from working in the sector because of a prior finding of Misconduct that is based on poor quality or incomplete investigative processes, inaccurate information, or relates to conduct that does not present a true safeguarding risk, such that an inability to work in the sector is disproportionate.	2	4	8	The Scheme requires participants to identify their internal definitions of Misconduct for the purpose of the Disclosure Statement which will enable requesting organisations to critically assess the information provided. Disclosing Organisations are expected to apply a materiality threshold to disclosing any finding of sexual harassment to a Requesting Organisation. If such conduct is considered to be of a nature that does not indicate a real safeguarding risk, they retain discretion not to disclose it and to document this decision. Participating Organisations are required, under the Scheme, to have in place robust, fair and reliable disciplinary procedures and to use technical measures to keep complete, accurate and reliable HR records, and processes for updating and reviewing records, in particular when facts linked to elements of the case have changed or been reassessed. Decisions made about - and on the basis of - Statements of Conduct are not automated and Participating Organisations are required to consider the representations of data subjects on the Statement of Conduct.	1	1	1	International HR HR Advice and casework

Statements of Conduct containing sensitive, confidential information are disclosed to unauthorised third parties, there is another type of data breach concerning the documents.	2	3	6	Statements of Conduct are only created and shared by Authorised Personnel within a Participating Organisation. Misconduct Histories will only be shared with using in a secure and encrypted manner, and accessed by, Authorised Personnel within a Participating Organisation. An up-to-date register of Participant Organisations and Authorised Personnel within such organisations will be maintained by the SCHR. The following security measures will be adopted encrypted in transit and at rest, password protection, encrypted files, restrictions on printing statements of conduct. If third party processors are used for data sharing these will be subject to GDPR- compliant contractual obligations. Completion of a Statement of Conduct and decision making on the basis of this document will be performed by dedicated HR Advisers. People Support will receive and share Statement of Conduct.	1	1	1	International HR HR Advice and casework People Support

Insufficient transparency for affected data subjects – i.e. data subjects do not understand how their data is used; with whom it will be shared; how decisions will be made based on the data; what rights they have in relation to the processing; and, in a complex controller arrangement) who is the duty bearer for these rights. The scheme could cause distress, or inappropriately deter applications for roles in the sector, if not adequately explained.	1	3	3	Clear information to be provided to affected or potentially affected data subjects through updates to privacy notices for employees and applicants. Access to the terms of the Scheme and copy of this DPIA to be made available. Clear information to be provided to all recruits (with access to an explanation of the Scheme and its terms of the Scheme available through the website) Internal communications in place to socialise existence of scheme to data subjects and provide contact point for questions and concerns: FAQs, policies on RedRoom, verbal presentation, recruitment procedure fully documented with new Scheme process.	1	1	1	Gaelle Pertot, International HR Project Adviser Steph Harris, Head of International HR HR Advice and casework
Too much data is shared by a responding Participating Organisation.	2	4	8	The Statement of Conduct form will include only official conclusions of reports and disciplinary processes (unless there are exceptional circumstances duly documented and adopting rights and principle based reasoning). The Scheme adopts a standardised Statement of Conduct form which requests only certain data required for the purposes of the Scheme, in order to facilitate data minimisation.	1	1	1	International HR HR Advice and casework

Information Commissioner's Office (ICO) Consultation

Based on the risk log and relevant mitigation plans outlined above, there are no residual high risks which will prevent the Scheme from continuing and need to be immediately raised with the ICO.

Each risk is mitigated effectively, and the overall severity of each respective risk is not high and is proportionate to the aims of the Scheme.

In the event of a data breach, the British Red Cross and the Information Asset Owner will comply with the internal policy requirements set out in the British Red Cross Incident Reporting policy,[2] accessible on the British Red Cross intranet, and the external regulatory requirements summarised by the ICO:

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. We must do this within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay.
- We should ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals
- We must also keep a record of any personal data breaches, regardless of whether we are required to notify.[3]

[2] British Red Cross Chief Executive Officer, *Incident Reporting Policy*, British Red Cross, <https://britishredcross.interactgo.com/Interact/Pages/Content/Document.aspx?id=1291&SearchId=>, Accessed 20/06/19

[3] "Personal Data Breaches". 2019. *Ico.Org.Uk*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/. Accessed 20/06/19.

Conclusion

Conclusion

The GDPR has been specifically taken into account in the development of the Scheme, and from a GDPR standpoint, implementing organisations consider that the lawful basis for processing personal data in this context is **the legitimate interests of the implementing organisations and, to a certain extent, the public interest of protecting potential victims.**

Moreover, many of the Scheme's principles around the processing of personal data and recommended processes to request, transfer and obtain such data are meant to bring the Scheme in line with GDPR requirements by ensuring fair, transparent and proportionate processing of data, protecting the information processed and maintaining the rights of data subjects.

One of the main ways of achieving fairness in the processing of hires' personal data is through transparency for the individuals whose information is processed. Data subjects will be informed, by their current employer, and as candidates, by their prospective employer, of the existence of the Scheme, and the modalities of its application.

As set out above, we consider that ay risks to the data subjects have been mitigated effectively, and the residual level of risk is proportionate to the aims of the Scheme.

Implementation of the Scheme contributes to organisations' work to prevent and address the consequences of sexual harassment and sexual exploitation and abuse in the humanitarian and development sector.

Organisations committed to this Scheme hope that it can be a good start and the basis from which to explore further collaborative approaches.

The Scheme is linked to other efforts to prevent sexual exploitation and abuse through the employment cycle, including the Interpol pilot of an international criminal vetting system for the Aid Sector and the FCDO-led Aid Worker Registration Scheme that is due to be piloted in 2020 which the BRC International Directorate might consider in future stages.

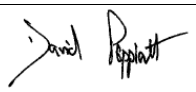
Review schedule

This document is subject to review every 3 years from sign-off date, unless there are any significant changes to the process such as:

Review schedule				
Date signed off	**Author**	**Next review date**	**Reviewed on**	**Reviewed by**
14/01/2021	Gaelle Pertot	3 years		

Sign-off

By signing the below, each signatory agrees with the conclusion of the full DPIA and that the Scheme meets all regulatory and internal requirements in terms of data protection and processing.

Required Signatories			
Name	**Role**	**Date**	**Signature**
Milgo Ali	Head of Information Governance and Data Protection Officer	14.01.2021	
David Peppiatt	Interim Executive Director of International Directorate	14.01.2021	

Appendices

Appendix 1 – Supporting documentation

Legitimate Interests Assessment

SCHR Misconduct Disclosure Scheme Le

Supporting documentation – Statement of Conduct Template

Click and type Date here

Private and Confidential
(to be completed by HR Department)

British Red Cross participates in the Inter-Agency Misconduct Disclosure Scheme. This Statement of Conduct adopts the definitions used in the Scheme.

STATEMENT OF CONDUCT – CONFIDENTIAL
This Statement is provided in answer to a request by (name), (title), (organisation)

1. Name of Candidate: xxxxxxxxxxxx

2. Duration of employment: from XX/XX/XX to XX/XX/XX

3. Was the Candidate found to have committed Misconduct (sexual exploitation, sexual abuse or sexual harassment) during the period of employment defined above?

(a) □ Yes
The nature of the Misconduct is: xxxxxxxxxxxx
(b) □ No
(c) □ I am unable to specify the nature of the Misconduct because of the following legal / regulatory requirements: xxxxxxxxxxxx

3.1. If the answer is **yes**, was a Disciplinary Measure imposed upon the Candidate?

(a) □ Yes, the Disciplinary Measure was xxxxxxxxxxxx
Date of Disciplinary Measure: XX/XX/XX
(b) □ No, for the following reasons: xxxxxxxxxxxx
(c) □ I cannot provide an answer to this question for the following reason(s):

3.2. Is the Candidate currently being investigated for an allegation of sexual exploitation, sexual abuse or sexual harassment?

(a) □ Yes
The nature of the Misconduct is:
(b) □ No
(c) □ I am unable to provide an answer

4. British Red Cross adopts the United Nations definitions of sexual exploitation, sexual abuse and sexual harassment.

Signature

Name and Title

Glossary & Acronyms

Term	Definition
HR	Human Resources
SCHR	Steering Committee for Humanitarian Response
GDPR	General Data Protection Regulation