**EQUALITY & HUMAN RIGHTS IMPACT ASSESSMENT (EHRIA)**

# EHRIA PUBLICATION

**Date:16/07/2020**

This is a summary of the key decisions/actions taken in the recent EHRIA, and has been separated from the full EHRIA document for publication on SCRA's external website in compliance with statutory requirements.

**The Scottish Children's Reporter Administration (SCRA) are pleased to publish the outcome of this Equalities and Human Rights Impact Assessment on:**

**The CSAS Security Policy**

The SCRA security policy for working with the Core Systems and Applications Solution (CSAS) is defined by the combination of 4 documents. These are:-

1. CSAS Security Policy V1.0 (Draft 0.3)
2. Security Operating Procedures (SyOps) for SCRA Users of CSAS (Draft 0.3)
3. Security Operating Procedures (SyOps) for Admin Users of CSAS (Draft 0.2)
4. The Addendum to the CSAS Security Policy

Only 2 of these documents are applicable to user, depending on the capacity in which the users is accessing CSAS. The security policy for a normal SCRA staff user of CSAS requires them to comply with (1) and (2) above, whereas for an SCRA staff performing admin tasks requires them to comply with (1) and (3).

CSAS consists of two tenancies, SCRA own the primary CSAS tenancy and CHS own the CHS tenancy. SCRA security policy for CSAS is only concerned about the CSAS tenancy.

The policy has been developed to ensure that personal details stored and processed on the system remain private and are only used to support the business function that they were supplied for.

The intended outcomes of the policy are:

- To demonstrate that SCRA is a safe custodian of case and volunteer data stored and processed within CSAS.

- To have distinct security policies in place for the 2 different types of SCRA user accessing CSAS.
- All authorised users of CSAS are security cleared and appropriately trained prior to being provided with access to SCRA's case information.
- To prevent unauthorised access to CSAS and disclosure of personal data stored within CSAS.
- Access to CSAS data is provided on a 'need to know' basis.
- To segregate OFFICIAL-SENSITIVE information assets from OFFICIAL information assets so appropriate security controls are in place to protect the information asset sets of different sensitivities.
- SCRA is the Data Controller of all case data and Data Processor of volunteer data working on CHS's behalf.
- To ensure that CHS staff and their volunteer community are able to get access to the specific case records they need to perform their role.
- To ensure the policy meets their current business requirements.

SCRA already has a system security policy and SyOPs in place for their Case Management System (CMS), so this provided a good place to start when developing the new policy. As CSAS is a cloud application comprising of two tenancies, accessible through the internet, there are considerable differences between the 2 systems that needed to be taken into account when drafting the new policy. Also a separate SyOps would be needed for the 2 different category of users, i.e. SCRA users and Admin users.

The Security and Information Governance (SIG) work stream has regular meetings with representation from CHS, Leidos and the Arcanum, the CSAS accreditor. The SIG meetings provided a suitable forum for discussing the requirements during policy development. Also the National Cyber Security Centre, as the authority on Cyber Security produce advice and guidance on a broad range of cyber security related topics, these were used where relevant.

After the policy was drafted consultation has taken place with:-

- HR Sub Group
- CSAS Security and Information Governance leads - Technical Leads, IG Leads.
- The CSAS accreditor (Arcanum).
- The Senior Information Risk Owners (SIROs) for both CHS and SCRA
- Organisation Readiness for subsections such as the development of the Role based access controls (RBAC)
- Digital Delivery Board members
- Scottish Government Digital First and Technical Assurance Framework assessors
-

Equalities Ambassadors will be consulted following initial completion of the EHRIA for the policy.

The evidence and legislation used to develop the policy were:

- Human Rights Act – specifically articles 2, 4-8
- Data protection legislation (GDPR)

- ISO 27001 as it is considered security best practice
- Disclosure of Information legislation.

**Impact:**

| **The Public Sector Equality Duty** | |
|---|---|
| **Will the impact and outcomes of the new or revised policy, practice or process:**<br>(Consider for children and young people referred in terms of the equality risk assessment of their journey through the hearing system including initial referral, investigation and decision, attendance and participation at hearings and related court proceedings.<br>Consider for staff in terms of the equality risk assessment for the staff journey with SCRA which includes recruitment, retention, progression, promotion, training etc.) | |
| **Contribute to eliminating discrimination, harassment and victimisation?**<br>**E.g.**<br>• Raise awareness of our SCRA's vision and values for equality, diversity and inclusion.<br>• Challenge appropriately any behaviours or procedures which do not value diversity and advance equality of opportunity | **POSITIVE:**<br>It will contribute to eliminating discrimination, harassment, victimisation ☒ |
| | **NO EFFECT:**<br>It will have no effect on discrimination, harassment and victimisation ☐ |
| | **NEGATIVE:**<br>It will make discrimination, harassment and victimisation worse ☐ |
| **Advance equality of opportunity between those who share a protected characteristic and those who do not?**<br>**E.g.**<br>• Remove or minimise disadvantage<br>• Meet the needs of equality groups that are different from the needs of others participation in public life | **POSITIVE:**<br>It will advance equality of opportunity ☐ |
| | **NO EFFECT:**<br>It will have no effect on equality of opportunity ☒ |
| | **NEGATIVE:**<br>It will reduce equality of opportunity ☐ |
| **Foster good relations between those who share a protected characteristic and those who do not? E.g.**<br>• Tackle prejudice<br>• Promote understanding | **POSITIVE:**<br>It will foster good relations ☒<br><br>Protecting the information of children and families is crucial and will be enhanced by this security policy. |
| | **NO EFFECT:**<br>It will have no effect on good relations ☐ |
| | **NEGATIVE:**<br>It will cause good relations to deteriorate ☐ |

| |
|---|
| It will uphold human rights articles. ☒ |

**With particular positive effects:**

| |
|---|
| ☒ **Age** (e.g. older people or younger people):<br>The Scottish Children's Hearings System is all about improving the lives of vulnerable children and the security of their data is paramount to this providing this service. |
| ☐ **Human rights compliance** (e.g. civil, political, economic, social, and cultural rights):<br><br>CSAS Users and children and families – articles 2, 4-8 will be positively impacted by the policy and procedures. |

**There are no negative effects.**

| |
|---|
| Recommended course of action: select relevant outcome and check the box when prompted: |
| **Outcome 1:** Proceed – no potential for unlawful discrimination/adverse impact on equality duty or interference with human rights has been identified.<br>☒ |

**SCRA Equality Review Group.**