Independent Child Trafficking Guardian

Data Protection Impact Assessment (DPIA)

1. Introduction

The aim of the Independent Child Trafficking Guardian (ICTG) service is to provide assistance, support and representation to a children and young people who are, or may be, a victim of the offence of human trafficking, or who are vulnerable to becoming a victim of human trafficking. The service will provide support to children and young people who arrive in Scotland unaccompanied and who will have undergone an arduous migration journey alone. Although these children will receive looked after status and receive local authority support, they face many wider challenges and additional support is therefore required. This can include going through the trafficking process, via the National Referral Mechanism, and in many cases, the asylum process as well. They also face further barriers such as breaks in their education, adapting to a new country, and learning a new language.

Establishment of ICTGs will fulfil the duty set out under Section 11 of the Human Trafficking and Exploitation (Scotland) Act 2015. ICTGs will work closely with other professionals when supporting a child or young person. The ICTG's role will be to draw together a network around each young person, with the aim of building close and productive relationships with other professionals. This will include social workers, lawyers and health care professionals. It is the intention that the functions of the ICTG must be such that they complement, rather than conflict or compete with, existing statutory roles. The ICTGs will focus on where they can add value in supporting these eligible children and address any gaps in support which are needed to meet their specific needs. These functions will be described in more detail within non-statutory guidance to be published.

The desired outcome is that every child or young person that needs support from an ICTG will be appointed one.

The National Outcomes which this policy contributes to are, that people:

- grow up loved, safe and respected so that they realise their full potential
- respect, protect and fulfil human rights and live free from discrimination

2. Document metadata

2.1 **Name of Project:** Independent Child Trafficking Guardian

2.2 **Author of report:** Robert Scott

2.3 **Date of report:** 11 01 2023

2.4 **Name of Information Asset Owner (IAO) of relevant business unit:** Tom McNamara

2.5 **Date for review of DPIA:** The DPIA will be reviewed in April 2024 once the ICTG service has been in place for a year .

Review date	Details of update	Completion date	Approval Date

3. Description of the project

3.1 Description of the work

ICTGs will be appointed to support children who may have been a victim of, or may be vulnerable to becoming a victim of, human trafficking, that have no parental guardian in the UK. Recognising that these children and young people are vulnerable, the ICTG will provide assistance and support in navigating the complex welfare, care, immigration, asylum, and trafficking systems, often in a foreign language. The ICTG can represent young people in engaging with the various authorities and speak on the child's behalf to avoid the need for them to re-live their experiences through constant re-telling of their story to different authorities.

Generally ICTGs will provide support to young people under the age of 18. However there are some circumstances where a young person will still be eligible to receive support from an ICTG after the age of 18.

ICTGs will work closely with other professionals when supporting a child or young person. The ICTGs role would be to draw together a network around each young person, with the aim of building close and productive relationships with other professionals. This would include social workers, lawyers and health care professionals. It is the intention that the functions of the ICTG must be such that they complement, rather than conflict or compete with, existing statutory roles. They should focus on where they can add value in supporting these eligible children and address any gaps in support which are needed to meet their specific needs.

3.2 Personal data to be processed

Variable	Data Source
Full details of child concerned, as available: name, date of birth, place of birth, home address in Scotland.	Personal data may be sourced from databases of statutory organisations, such as Police Scotland, Health, Education, Social Work. It is good practice to have data sharing agreements in place, where required: Data sharing agreements | ICO The views of and input from the child concerned may also be sought, using age-appropriate language and taking into account the vulnerability of the child.
Details of professionals working with children and young people: name, place of work.	Personal data may be sourced from databases of statutory organisations, such as Police Scotland, Health, Education, Social Work, and also professional bodies and third sector organisations.

	It is good practice to have data sharing agreements in place, where required: Data sharing agreements | ICO
Special category data of child concerned – see detail at 5.5 below	Data may be sourced from databases of statutory organisations, such as Police Scotland, Health, Education, Social Work. It is good practice to have data sharing agreements in place, where required: Data sharing agreements | ICO The views of and input from the child concerned may also be sought, using age-appropriate language and taking into account the vulnerability of the child.

3.3 Describe how this data will be processed

ICTG work will encompass processes for safeguarding and protecting children from harm, and inter-agency child protection procedures are defined for circumstances in which a child may have experienced or may be at risk of significant harm.

The National Guidance for Child Protection in Scotland highlights key principles relevant to practice in these areas, making it clear that sharing relevant information is an essential part of protecting children from harm. However, information shared must only be that which is necessary for child protection purposes.

Practitioners and managers in statutory services and the voluntary sector should all understand when and how they may share information. Practitioners must be supported and guided in working within and applying the law through organisational procedures and supervisory processes. Within agencies, data controllers and information governance/data protection leads should ensure that the systems and procedures for which they share accountability provide an effective framework for lawful, fair and transparent information sharing. Where appropriate, data sharing agreements must be in place.

Where there is a child protection concern, relevant information should be shared with Police or Social Work without delay, provided it is necessary, proportionate and lawful to do so. The lawful basis for sharing information should be identified and recorded. Agency data protection leads should be able to advise where doubt about lawful basis exists.

When in doubt about the boundaries of information sharing, practitioners are advised to seek advice from their line managers. Further consultation may be necessary with agency advisors for Getting it right for every child (GIRFEC) and/or child protection. There should also be a governance lead to consult about the sharing of information in principle, without disclosing the identity of the individual. In any circumstances, agreement or disagreement and course of action or intervention should be recorded.

Special category data may be shared if this is necessary to safeguard individuals or types of individuals at risk from neglect or physical, mental or emotional harm, or in order to safeguard the physical, mental or emotional well-being of an individual, when the individual is under 18, or aged 18 or over and at risk. (A person over 18 years may be, 'at risk' if they have needs for care and support; or are experiencing, or at risk of, neglect or physical, mental or emotional harm, and as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk

of it: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/18/). Such data includes racial or ethnic origin; data concerning health; sexual orientation or sex life; political opinions; religious or philosophical beliefs; trade union membership; genetic data; or biometric data (where used for identification purposes).

Article 9(2)(h) of UK GDPR, Article 9(2)(h) permits the processing of special category data if it is necessary for *inter alia* the provision of health or social care, under Schedule 1, condition 2 of the Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1.

3.4 Explain the legal basis for the sharing with internal or external partners

In relation to UK Data Protection Law, the GDPR has been incorporated into UK data protection law as the 'UK GDPR', which is in force alongside the Data Protection Act 2018. Guide to the UK General Data Protection Regulation (UK GDPR) | ICO

Section 3.3 above outlines the approach to supporting agencies in applying data protection principles within the law.

In terms of child protection, there are overarching duties which prescribe many of the duties and corresponding powers of relevant authorities. These include, but are not limited to, the following:

- duty to investigate and report issues in relation to child protection, in terms of the Police and Fire Reform (Scotland) Act 2012 and the Children's Hearings (Scotland) Act 2011
- duty to promote social welfare, in terms of the Social Work (Scotland) Act 1968 and the Children (Scotland) Act 1995.

In terms of the provision of social care, the processing of special category data has a lawful basis under the Children and Young People (Scotland) Act 2014: https://www.legislation.gov.uk/asp/2014/8/part/11/enacted.

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish Refugee Council Aberlour Children's Charity	Scottish Guardianship Service (Current non-statutory provider)
Aberdeen City Council Just Right Scotland Barnardo's Scotland British Red Cross CARE Centre of Excellence for Children's Care and Protection (CELCIS) Clackmannanshire and Stirling Child Protection Committee Convention of Scottish Local Authorities (COSLA) Edinburgh Child Protection Committee	Response to consultation (interest in terms of child protection and UASC)

Educational Institute of Scotland (EIS) Glasgow City Health and Social Care Partnership Highland Child Protection Committee NHS Tayside Scottish Guardianship Service (SGS) (Scottish Refugee Council & Aberlour) Scottish Association of Social Work Social Work Scotland South Lanarkshire Council	

4.2 Method used to consult with these groups when making the DPIA.

Regular meetings have been held between the Scottish Government and the Scottish Guardianship Service, including discussions on provision of the ICTG. The latter fed into the development of this impact assessment.

Consultation to seek views on the appointment, role and functions of the ICTG and wider operational issues opened on 26 August 2019 and closed on 17 November 2019. Analysis of the 40 responses received has been carefully considered by the Scottish Government.

4.3 Method used to communicate the outcomes of the DPIA.

The DPIA will be published on the Scottish Government website and shared directly with the organisation appointed to manage this service.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

Scottish Government will have no direct involvement but processes within the ICTG service may require that data is shared between organisations involved in child protection, including statutory authorities, for example local authority social work and education departments, Police Scotland, NHS, and service providers in the third sector.

The organisation appointed to manage this service will ensure that all data processed will be in compliance with data protection legislation and in compliance with the respective organisations' information management and information sharing processes and procedures.

The organisation appointed through the procurement process to run the ICTG service will be the data controller and data processor, and ICTGs will be data processors.

5.2 Anonymity and pseudonymity

The organisation appointed to manage this service will not share any personal data with partners without the data subjects' express consent, unless they are under a legal obligation obligation to do so due to safeguarding concerns. For instance, where there is a child protection concern, relevant information should be shared with police or social work without delay, provided it is necessary, proportionate and lawful to do so.

5.3 Technology

The organisation appointed to manage this service will apply their own information management processes to the data processed and shared electronically.

5.4 Identification methods

The organisation appointed to manage this service will apply their own information management processes to the data processed for this purpose.

5.5 Sensitive/Special Category personal data

The organisation appointed to manage this service will ensure that special category data is only shared if this is necessary to safeguard individuals or types of individuals at risk from neglect or physical, mental or emotional harm, or in order to safeguard the physical, mental or emotional well-being of an individual, when the individual is under 18, or aged 18 or over and at risk.

A person over 18 years may be 'at risk' if they have needs for care and support; or are experiencing, or at risk of, neglect or physical, mental or emotional harm, and as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/18/.

Such data includes racial or ethnic origin; data concerning health; sexual orientation or sex life; political opinions; religious or philosophical beliefs; trade union membership; genetic data; or biometric data (where used for identification purposes).

Additionally, article 9(2)(h) of UK GDPR, Article 9(2)(h) permits the processing of special category data if it is necessary for *inter alia* the provision of health or social care, under Schedule 1, condition 2 of the Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/schedule/1

5.6 Changes to data handling procedures

Scottish Government will not process any personal data for the purpose of progressing this service.

The organisation appointed to manage this service will ensure that all data processed will be in compliance with data protection legislation and follow their own information management processes.

The organisation appointed to manage this service will ensure that there are processes for enabling any individual wishing to access their personal data to do so. The organisation will not share any personal data with external partners without the data subjects' express consent unless they are under an legal obligation to do so.

5.7 Statutory exemptions/protection

Where there may be a child protection concern, information may be lawfully shared among statutory authorities without the need for consent to be given by the individual(s) to whom the information relates (see 3.3 and 5.5).

5.8 Justification

Substantial Public Interest Conditions / Safeguarding of Children at Risk

5.9 Other risks

It is recognised that the cyber risk profile for this work is high. Questions addressing this risk were part of the Invitation to Tender to appoint an ICTG service provider, and responses from tenderers were required to demonstrate their organisation's approach to Information Security and the controls that are in place to protect the processing of information and ensure continuity of the service offered.

6. General Data Protection Regulation (GDPR) Principles

Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	See section 3.4. Data controllers should always be transparent and fair with how they use the data, with particular concern given to the sensitive nature or context. In certain circumstances data may, if the responsible data controller deems appropriate in the given situation, be transferred under the 'public task' or 'vital interests' bases, or with the written consent of the individual or their legal guardian, where that consent is "fully informed" and deemed valid.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.2 Principle 2 – purpose limitation	Yes	The information collected and shared by the appointed organisation will only be what is necessary to provide the protection and/or support that the child requires.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.3 Principle 3 – adequacy, relevance and data minimisation	Yes	The information processed will be proportionate to what is necessary to provide the protection and/or that the child requires.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.4 Principle 4 – accurate, kept up to date, deletion	Yes	Any inaccurate data in the appointed organisation's documentation will be corrected or removed at the data subject's request.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes	The data will only be kept for as long as outlined in the appointed organisation's data retention policies, and anonymized where required.

		More information on anonymization here: anonymisation-intro-and-first-chapter.pdf (ico.org.uk)
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.6 UK GDPR Articles 12-22 – data subject rights	Yes	The appointed organisation will have procedures in place to ensure data subjects are able to exercise their rights as required by data protection legislation.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.7 Principle 6 - security	Yes	The appointed organisation will have appropriate security measures in place to protect personal data as required by legislation.
Principle	**Compliant – Yes/No**	**Description of how you have complied**
6.8 UK GDPR Article 44 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	No	The appointed organisation will be bound to comply with data protection legislation and will not share or transfer personal data, stored within their information management systems, to a country or territory outside the EEA. However, the need to share information outside of the EEA may come up very infrequently and the considerations around it can be complex. This should be managed on a case-by-case basis by the Guardian in discussion with their line manager and any decisions taken should be informed by: 1. the needs of the child or young person; 2. the organisation that information is to be shared with and any rules governing their systems, in the attempt to verify the legitimacy of a service; and 3. what is known from County of Origin Information about the risk that a state could intercept communications and any risks that may carry for the child or for a relative still in the country of origin. For example, Eritrea, China and Iran are particularly high risk countries in that respect. Transfers of data to and from the UK must be protected by an adequacy agreement with the recipient country, or an additional safeguard. More detail can be found here: International transfers after the UK exit from the EU Implementation Period | ICO

7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
The Scottish Government has no control over the appointed organisation's information management systems.		Reliance that the appointed organisation adheres to all relevant data protection legislation.	Accept
The Scottish Government has no control over information sharing by the appointed organisation.		Reliance on the appointed organisation that 1. Their staff are trained to ensure compliance with their responsibilities. 2. They are aware that further information may be sought via the ICO's Data Sharing Code of Practice: https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/	Accept
Management of correspondence related to the ICTG service by the Scottish Government which may contain personal information		Scottish Government staff will adhere to all relevant data protection legislation and follow internal processes. Mandatory data protection training is undertaken annually.	Accept

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Data processed by the appointed organisation	PR1	Advice to the appointed organisation that their information management processes must adhere to all relevant data protection legislation. The appointed organisation is accountable for internal responsibilities in terms of self-evaluation of systems and practice, including in relation to	Robert Scott

		data protection and processing of information.	
Incorrect information sharing	PR2	Advice to the appointed organisation that their staff must be appropriately trained and supported to ensure compliance with their responsibilities.	Robert Scott

9. Data Protection Officer (DPO)

The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action

10. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of providing the ICTG service has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	Date each version authorised
Tom McNamara DD: Children's Rights, Protection and Justice	