# DATA MANAGEMENT POLICY AND GUIDANCE FOR SAFEGUARDERS

# Contents

# Introduction

## The GDPR and the Data Protection Act 2018

Due to the nature of the Safeguarder's role every Safeguarder must comply with the European Union (EU)'s General Data Protection Regulation (GDPR). A Safeguarder must also register as a 'data controller' with the Information Commissioner's Office (ICO), which is the UK's 'supervisory authority' for purposes of the GDPR. These are contractual obligations which flows from the terms of their appointment by Scottish Ministers as contained in each Safeguarder's letter of appointment.

The GDPR supersedes the Data Protection Act 1998 ('the DPA 1998') and has immediate effect in the UK from 25 May 2018. Furthermore, the UK Parliament has finally passed the new Data Protection Act 2018 (DPA 2018) which received Royal Assent on on 23 May 2018. Rather than simply replicating the GDPR (which is not necessary for the GDPR to have effect in UK law) the new DPA 2018 primarily makes provision for how the UK will exercise the discretion allowed to it by the EU when implementing the GDPR. The DPA 2018 also explicitly repeals the DPA 1998.

Safeguarders who are registered with the ICO on 25 May 2018 do not need to re-register until their current registration expires.

The GDPR is specifically concerned with 'personal data' (the definition of which is noted further on in this document) rather than 'data' in the widest sense. The GDPR uses the word 'process' to describe what people do with personal data. In discharging their role, Safeguarders will 'process' personal data of various kinds from various sources. The kind of personal data that they process will fall under the provisions of the GDPR. Put very simply 'process' means 'collect/receive and use' but the full definition of 'processing' in the GDPR at Article 4(2) reads as follows:

> "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*

There are some exemptions for Safeguarders to the need to comply with the GDPR. These are set out in detail at the end of this introduction.

## The Children's Hearings (Scotland) Act 2011 Rules of Procedure

In the Children's Hearings (Scotland) Act 2011 (Rules of Procedure in Children's Hearings) Rules 2013, Rule 9 outlines the duties of the Safeguarder in respect of information and documents under the 2011 Act (i.e. alongside what anything else, like the GDPR, may require) as follows:

> *"(1) Any documents which are given to a Safeguarder by the Reporter under, or by virtue of, the Act or any other enactment must be kept securely in the Safeguarder's custody and returned to the Reporter on the termination of the Safeguarder's appointment.*
>
> *(2) The Safeguarder must not cause or permit any information which they have obtained by virtue of their appointment as a Safeguarder under the Act to be disclosed, except as permitted by virtue of the Act or any other enactment".*

## The Practice Standards for Safeguarders

Practice Standard 5: Confidentiality sets out what is expected of Safeguarders in this regard:

> *"A Safeguarder will maintain confidentiality and shall not disclose information unless in accordance with the law".*

Practice Standard 5 is set out in full at Appendix 1.

## This Guidance

The purpose of this guidance is assist Safeguarders to comply with their data management responsibilities under:

- The GDPR and the DPA 2018
- The Children's Hearings (Scotland) Act Rules of Procedure
- The Practice Standards for Safeguarders

This guidance has been written in recognition of the fact that the safeguarding role is unique and that the way that Safeguarders handle data is somewhat atypical in comparison with other roles affected by the GDPR and the DPA 2018. There was a risk that the particulars of the safeguarding role may cause some concern amongst Safeguarders as to how they should approach compliance with the GDPR and the DPA 2018. This guidance seeks to lessen that risk.

This guidance is not and can never be a substitute for guidance or direct advice from the ICO, nor should this guidance be relied upon as legal advice. For the purposes of regulation of data controllers, the relationship in the UK is between that Safeguarder, as a data controller, and the ICO. The responsibility for compliance with the data protection regime in force at any given time is therefore the responsibility of the Safeguarder. It is not the responsibility of Scottish Ministers or Scottish Government or of the Safeguarders Panel Team, currently operated on behalf of Scottish Ministers by Children 1st.

The guidance covers:

1. The data to which the GDPR applies ('personal data' & 'special category personal data')
2. The new data protection principles and the lawful bases on which data may be processed
3. Data Protection Impact Assessments (DPIA)
4. Records of processing
5. Privacy notices
6. Data retention and destruction policy
7. Data breach
8. Data storage and transmission including use of encrypted memory sticks
9. Using secure email (CJSM)
10. Registering as a data controller
11. Summary

It has five appendices:

1. Practice Standard 5: Confidentiality
2. Privacy Notice Template
3. How to register as a Data Controller with ICO
4. How to use a memory stick that is compatible with Microsoft Windows software

## Exemptions to the Need to Comply with the GDPR for Safeguarders

The DPA 2018 allows for Safeguarders not to comply with parts of the GDPR, in relation to individual rights, in certain circumstances. Individual rights appear in Part 3 of the DPA 2018 ('Rights of the data subject'). The exemptions work by way of Schedule 3 of the DPA 2018 and Safeguarders are named explicitly at Schedule 3, Part 2, Paragraph 8 (q) (iii). These provisions of the DPA 2018 are complex but an attempt to simplify them follows. These exemptions are particularly relevant to section 5 of this guidance, on privacy notices.

## What the Data Subject (Definition Below in Section One) Expects and Wants

If a person attempting to exercise a right in law to request data, requests that a Safeguarder share data which the Safeguarder is 'processing' (see definition in Section 1 below) AND

- the data subject is under sixteen AND the person making the request has parental responsibilities for the data subject (in other words, this will usually mean a parent asking for data about their child or another individual under 16 for whom they are responsible) OR

- the data subject lacks capacity to deal with their own affairs AND the person making the request has been appointed by a court to manage those affairs.

the Safeguarder does NOT have to:

- provide information that would amount in terms of this guidance to a privacy notice (under Article 13 or under Article 14)
- provide information about that data processing or give access to that data to the data subject (Article 15) (and therefore does not have to provide it in a format that makes it easy for the data subject to pass it on (Article 20)
- change the data (Article 16)
- destroy the data (Article 17)
- only use the data for certain purposes (i.e. 'restriction of processing' (Article 18)) or not to use it at all objections to processing (Article 21)
- ensure compliance with the data protection principles under Article 5 in relation to the above (this rather circular provision is included because, technically, if you are exempt from the data protection principles in certain circumstances, then in those circumstances you can't be held to be subject to the data protection principles!)

BUT ONLY IF

- the data subject gave the Safeguarder the information expecting that it would not be shared with the person making the request

- the data was obtained during an examination or investigation to which the data subject consented expecting that it would not be shared with the person making the request
- the data subject has ‘expressly indicated’ that they do not want the data shared with the person making the request

## Serious Harm to the Data Subject

If providing information about data processing or giving access to that data to the data subject (under Article 15) would prejudice the carrying out of the Safeguarder’s function because it would blikely to cause serious harm to the physical or mental health of the data subject or another individual, the Safeguarder does NOT have to:

- provide information about that data processing or give access to that data to the data subject (Article 15)

# 1. The Data to Which the GDPR Applies ('Personal Data' and 'Special Categories of Personal Data')

The GDPR is concerned with 'personal data' not simply 'data'. Some subcategories of 'personal data' might be thought to be more sensitive than others and the GDPR calls these 'special categories of personal data'. Generally, processing special categories of personal data is prohibited but there is a list of exceptions to this prohibition and the role of the Safeguarder falls under at least one of them (as is made clear below). That means that Safeguarders will inevitably end up 'processing' *both* 'personal data' *and* 'special categories of personal data'.

'Personal data' is defined at Article 4(1) of the GDPR:

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

'Special categories of personal data' is defined at Article 9(1):

> *"…personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation…"*
>
> While criminal conviction data (including information about alleged criminal convictions) is not listed as a special category of personal data in the GDPR, the DPA 2018 confirms that criminal convictions data should be treated as special category personal data.

'Personal data' and 'special categories of personal data' can include:

- a single piece of data or a collection of data, including a collection that comprises evidence of an activity or decision;
- a narrative of how a Safeguarder went about their role or why a particular decision or recommendation was made.

It is also important to recognise that data (whether recorded and stored on paper or otherwise in 'hard copy' or electronically) can come in a number of different guises, for example:

- correspondence (letters, texts, emails etc.)
- notes of meetings, discussions and telephone calls, including taped/ digital recordings
- Safeguarder reports
- reports from other people or bodies
- legal advice received by Safeguarders when they are legally represented

Given the nature of the Safeguarder's role, it may be sensible to construe all data in a case as *potentially* classifiable as 'personal data' and treat it accordingly. This is not as onerous as it may sound, as will subsequently become clear.

In summary, Safeguarders will process personal data and special categories of personal data and must understand these terms and what forms 'data' can take.

## 2. The New Data Protection Principles and the Lawful Bases on Which Data may be Processed

The data protection principles in the DPA 1998 have been updated for the GDPR. There used to be eight, now there are seven, although in some documents that Safeguarders may come across reference may only be made to six. That is presumably because six of them are set out at Article 5(1) with one more set out at Article 5(2). In any case, the ICO refers to seven principles and this document does the same.

*"Personal data shall be*

a) *processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')*
b) *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')*
c) *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*
d) *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*
e) *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*
f) *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".*

And finally that

- *"The controller shall be responsible for, and be able to demonstrate compliance with, [these principles] ('accountability')".*

They may appear to be a little involved but consider looking at the way the GDPR itself summarises the seven revised principles:

1) lawfulness, fairness and transparency
2) purpose limitation
3) data minimisation
4) accuracy
5) storage limitation
6) integrity and confidentiality
7) accountability

Looked at this way it is clear that the principles really just amount to a requirement for data controllers to treat data in accordance with the reasonable expectation of the average citizen to privacy.

As an aid to simplification and understanding, it may help to consider how the opposite to the above would read and to ask yourself whether you would wish anyone to treat data about you in the following ways:

- unlawfully, unfairly and secretively
- for any purpose
- to the extent of any amount of information about you, limited only by how much they could get hold of
- with no regard for accuracy
- without limit of time
- careless as to damage or loss to you and similarly careless to anyone else finding out anything or everything about you, despite the fact they have no business doing so
- to be able to get away with all of that without anyone pulling them up about it

These 'negatives' of the principles help show the potential negative effects on an individual or individuals of a failure to process their data properly.

The seven principles deal with *how* data must be processed. They assume that a data controller is *allowed* to process it. A data controller is only allowed to process data on a 'lawful basis'. The lawful bases for processing are set out in Article 6 of the GDPR.The ICO website explains them as follows:

> *"At least one of these must apply whenever you process personal data:*
>
> *a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.*
> *b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.*
> *c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).*
> *d) Vital interests: the processing is necessary to protect someone's life.*
> *e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.*
> *f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)"*

For Safeguarders, the legal framework in which they operate means that typically (e) and/or (but atypically) (c) will provide the lawful basis for their work.

However, Safeguarders cannot *assume* that *all* the processing of personal data that they undertake whilst acting as a Safeguarder is capable of being justified on a lawful basis simply because of the nature of the role. As data controllers they would, if asked, need to be able to explain the lawful basis for any act of 'processing' they had undertaken *as well as* being able to demonstrate that the processing had been undertaken in accordance with the seven data processing principles.

In practice this is unlikely to present any practical problems for Safeguarders but it is a point on which caution should be exercised.

When it comes to 'special categories of personal data' most of the categories are unlikely to require to be 'processed' by a Safeguarder because they will not be relevant to the proper discharge of the Safeguarder's role. Insofar as such data might need to be processed, that data will probably already be known to the Hearing or Court (e.g. ethnic origin, data concerning health, sexual orientation). However, some ''special categories of personal data' will be contained in data provided to the Safeguarder via sources other than the data subject him or herself (e.g. in a social work report that contains information about the data subject) and the receipt and use of that data by the Safeguarder means that the Safeguarder is 'processing' it.

If a Safeguarder does have to process 'special categories of personal data', whether sourced from the data subject or from another source (for example because the issue of a child's ethnic origin was crucial to the Safeguarder's recommendations) the exemption (to the usual requirements) upon which it appears most Safeguarders would be able to rely is set out at Article 9 (2)(g):

- *"processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".*

This is because

- the work of the Children's Hearing System and the related the activity of the courts is undertaken in the public interest as well as in the interests of individual children
- the Safeguarders role has a clear basis in law
- Safeguarders do not process personal data for any other purposes than that for which it is collected (and so is 'proportionate to the aim pursued')
- Safeguarders are not only data controllers, registered with the ICO, they are also subject to the Practice Standards which lock in 'respect (for) the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject'
- the DPA 2018 confirms in paragraphs 18 and 19 of Part 2 of Schedule 1 that processing special categories of personal data for the purposes of protecting someone under the age of 18 from neglect or physical, mental emotional harm in circumstances where it is not appropriate to ask for consent is necessary for reasons of substantial public interest

A note in Article 12

- This article sets out the need for information to be provided in an 'easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child' and also deals with timescales for the provision of information. Safeguarders should familiarise themselves with it.

In summary, Safeguarders must

- only process personal data if they have a lawful basis to do so
- process *all* 'personal data' in accordance with the seven principles
- only process 'special categories of personal data' if they really need to in order to properly discharge their role and they if can pinpoint the legal basis (which will most likely be the public function or substantial public interest for special category personal data) which applies to that processing

## 3. Data Protection Impact Assessments (DPIA)

A DPIA is effectively a risk assessment made by a data controller of the risk to the data subject of a breach by the data controller. The GDPR deals with DPIAs at Articles 35 and 36. The wording in Article 35 is not quite clear and it may lead one to conclude that a Safeguarder does not process data in a way that would require the Safeguarder to produce a DPIA. This is because the wording is concerned with the 'scope' of processing as much as it is with 'high risk' of harm resulting from a data breach.

Safeguarders should not become over-concerned on this point. The GDPR compels the ICO to "establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment" and the ICO has done so. Their list is available at the link below, along with plenty of other relevant information about DPIAs

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

The existence of the ICO list means that it doesn't really matter whether there is any lack of clarity in what the GDPR itself says. If 'the kind of processing operations' that a data controller does are on the list that data controller needs to do a DPIA.

The list comes in two parts:

- *"We always carry out a DPIA if we plan to…* [lists activities]*"*
- *"We consider carrying out a DPIA if we plan to carry out any other…* [lists activities]*"*

Most of the items on both lists are very obviously not applicable to the Safeguarder role. However some arguably are, as follows, and in the absence of any definitive decision of a court on a Safeguarder's role vis-à-vis DPIAs it would seem sensible for Safeguarders to prepare one. There is a draft template DPIA on the ICO website here (please note this template may be subject to change by the ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/

Below are items drawn from the first ICO list ("We always carry out a DPIA if we plan to…") that appear to be those under which data processing by a Safeguarder would be most likely to fall, with illustrative examples.

- *"Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit."*
    - It is very arguable that a Safeguarder may, on occasion, have to use 'special category data' in order to help a Hearing or Court's decision-making as to a service or benefit that a child may require.

- *"Combine, compare or match data from multiple sources."*
    - Whilst, when set in context, this item clearly envisages automated, large-scale, data combination and comparison, the plain meaning of its words could apply to the task that a Safeguarder undertakes when they synthesise, in their report, elements of the contents of several other reports about, and interviews with, the child or children and the other people involved in the case.

- *"Process personal data which could result in a risk of physical harm in the event of a security breach."*
    - It is rare that physical harm to anyone would be the likely result of a Safeguarder's data breach but this is clearly possible. For example, a Safeguarder's report contains a note that a child lives with her aunt but does not contain the aunt's address. The child only has one aunt. The father who has abused the child and does not know where the child currently lives gets hold of a copy of the report as a result of a data breach by the Safeguarder. He is easily able to work out where the child lives because he knows there is only one aunt and he knows her address. He turns up at that address and physically harms both child and aunt.

The *purpose* of a DPIA is twofold:

1) to ensure that data controllers have given proper consideration to the risks associated with their processing, have taken steps to mitigate those risks and can make that information available to anyone who may ask for it to reassure them that the data controller is processing data appropriately
2) submission of the DPIA to the ICO and consequent feedback from the ICO provides reassurance to the data controller that they are processing data appropriately and can begin (or can continue) to process that data.

However, with respect to purpose two, the ICO guidance says that:

- *"If you have carried out a DPIA that identifies a high risk, and you cannot take any measures to reduce this risk, you need to consult the ICO. You cannot go ahead with the processing until you have done so."*

This is very helpful to Safeguarders because the measures that a Safeguarder would need to take to reduce risk in this context are *locked into* the Practice Standards for Safeguarders. Therefore if a Safeguarder meets the Practice Standards they will have adequately reduced the risk. That reduction means that they do not need to consult the ICO or obtain the ICO's approval before processing data.

An obvious question thereby arises: if a Safeguarder does not have to submit their DPIA to the ICO then

- how will anyone know that the Safeguarder has done one and
- when will it ever be needed?

The answers are

- They won't…
- …until there's a breach, in which case the ICO (to whom all breaches that are likely 'to result in a risk to the rights and freedoms of natural persons' must be reported) may ask to see it to help them decide the extent to which the data controller who has committed the breach is at fault (Children 1st has confirmed with the ICO that this is how it would work).

In summary, although strictly speaking Safeguarders may not require to produce a DPIA, as a matter of good practice, and to help protect themselves in the event of a data breach, Safeguarders should, nevertheless produce a *simple* DPIA. Conducting a DPIA, keeping a record of having done so and regularly reviewing it also helps to meet the seventh data protection principle ('accountability').

## 4. Records of Processing

The requirement to keep records is set out at Article 30. There is a 'derogation' from the provisions of the Article for 'an enterprise or an organisation employing fewer than 250 persons', which would appear to cover Safeguarders. However, Article 30(5) makes it clear that this derogation does *not* apply if:

- *"the processing (that the data controller) carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."*

The nature of the Safeguarder's role means that their processing could very easily be said to fall under one or more of those provisions.

Therefore, to minimise risk, Safeguarders should keep appropriate records. The good news is that, because the tasks that a Safeguarder undertakes are relatively uniform across every case, compliance is straightforward and the schema shown below in the table should be capable of applying to all of a Safeguarder's cases. If you imagine there being one record per case, for each case the first column below would be the headings and the second column below would be what appeared under each heading. Together they would comprise a cover sheet for a set of case papers. It will be readily observable that the same cover sheet would apply in every case.

It should be appreciated that there are only ever four processes during which a Safeguarder should ever be in possession of personal data in connection with their role:

1) During the case
2) For the purposes of report sampling
3) During a concern raised about a Safeguarder
4) During another process to which the Safeguarder becomes subject and which necessitates the possession of such personal data (e.g. a child protection concern, a police investigation)

In the case of the first three of these processes, there should never be any need for a Safeguarder to hold personal data about others outwith the time periods that apply to those data and these periods are typically relatively short. However, a Safeguarder's cases can sometimes go on for a long time and, in any case, during any one of the first three processes the relevant papers that the Safeguarder holds, insofar as they contain 'personal data', will count as 'records' and must therefore be kept in the prescribed manner.

The fourth category of process is beyond the scope of this guidance.

| Which records Article 30 requires to be kept: | What information should a Safeguarder provide: |
|---|---|
| 1(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; | The name and contact details of the Safeguarder (obviously this 'blank' will have to be filled in per Safeguarder). |
| 1(b) the purposes of the processing; | The purpose is to comply with the requirements of the Safeguarder's role as mandated and set out by the Children's Hearings (Scotland) Act 2011 and attendant regulations and including the resulting Practice Standards for Safeguarders. |
| 1(c) a description of the categories of data subjects and of the categories of personal data; | Categories of data subjects:<br>• Child/children<br>• Parents/carers/relatives/relevant persons<br>• Professionals involved (e.g. social workers, teachers)<br><br>Categories of personal data:<br>• Name and contact details<br>• Description of prior and present actions and views in relation to the matters with which the case at hand is concerned and supporting details as set out in the Safeguarder's report or reports to the Hearing or Court<br>• Reports from third parties (e.g. social work) |
| 1(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; | Categories of recipients<br>• Child/children<br>• Parents/carers/relatives<br>• 'Relevant persons' within the meaning of the Children's Hearings (Scotland) Act 2011<br>• Professionals involved (e.g. social workers, teachers, lawyers)<br>• The Hearing (i.e. panel members)<br>• The Court<br>• SCRA and its employees<br>• CHS and its employees<br>• The Safeguarders Panel Team (SPT) and its employees |
| 1(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; | N/A to Safeguarders |

| | |
|---|---|
| 1(f) where possible, the envisaged time limits for erasure of the different categories of data; | The data shall be processed no sooner than from the date of the Safeguarder's appointment and said processing will cease as soon as is practicable after the date of the occurrence of one or more of the termination events referred to in the Children's Hearings (Scotland) Act 2011 (Safeguarders: Further Provision) Regulations 2012 (No.336), at which point it will either be returned to the source from which it was obtained (which may mean the SPT) or be securely destroyed.<br><br>***A note on report sampling:***<br>When a Safeguarder is provided with a copy of any report *of which they are the author* for a purpose other than the use by the Safeguarder of said report in a case before the Children's Hearing or the Court the Safeguarder shall return that copy to the source from which it came (which in this case will mean the SPT) or, if that is not possible, securely destroy that copy in all and any formats as soon as is practicable after the date at which the purpose for which the report was provided has been completely discharged.<br><br>In the particular case that a Safeguarder is provided with such a report by the SPT for the purposes of 'report sampling' as part of the Performance Support and Monitoring Framework applicable to Safeguarders and as permitted by law; the date at which the purpose for which the report was provided has been completely discharged is normally the date no later than ten working days from the date of the meeting between the Safeguarder and the Safeguarders Panel Team at which the report was discussed.<br><br>Any retention of the report subsequent to the time period referred to above, without apparent justification, may be considered a data breach in terms of the data protection regime which the Safeguarders Panel Team may be obliged to report to the Information Commissioner's Office (ICO).<br><br>***A note on concerns:***<br>When a Safeguarder is provided with a copy of any material pertaining to a concern about that Safeguarder and which contains personal data the Safeguarder shall return that copy to the source from which it came (which in this case will mean the SPT) or, if that is not possible, securely destroy that copy in all and any formats as soon as is practicable after the date at which the concern has been completely resolved. |

| | |
|---|---|
| | The date at which the concern has been completely resolved is normally the date no later than ten working days after whichever of the following dates has most latterly occurred:<br>• The end of the period within which a Safeguarder may request a review of the outcome of a concern, that date being a date within twenty working days of the date on the 'concern outcome letter' as sent to the Safeguarder, without any such review being requested.<br>• When a review of the outcome of a concern having been requested has been completed, the date on the 'concern review outcome letter' as sent to the Safeguarder.<br><br>Any retention of the material subsequent to the time period referred to above, without apparent justification, may be considered a data breach in terms of the data protection regime, which the Safeguarders Panel Team may be obliged to report to the Information Commissioner's Office (ICO).<br><br>***A note on other processes:***<br>These will follow timescales of their own and the Safeguarder should refer to those operating those processes and/or the ICO for advice. |
| 1 (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | Reference to this guidance and to Practice Standard 5 of the Practice Standards for Safeguarders should be made. |

In summary, a Safeguarder must keep records of the type of personal data that they hold but only for the period for which they actually need to hold the personal data to which the records relate. After that period has ended the data must be securely destroyed immediately or within a certain timescale. Once it has been destroyed there is obviously no data held by the Safeguarder to which a record of the type of data held can relate. Consequently there is no need to keep a record of the type of data held unless it is actually *being* held. In any case, data that is being held may need to be made available to the ICO for inspection on request.

# 5. Privacy Notices

A privacy notice (PN) is one of the terms given to the document in which a data controller gives the person whose data they are processing (the 'data subject') information about that processing. Other terms for this type of document include 'fair processing notices' and privacy policies', however all of these terms can be used interchangeably and all serve the same legal function – which is to comply with Articles 13 or 14 of the GDPR. The information they must give is set out at Articles 13 or 14 of the GDPR. Article 13 applies where data is obtained *directly* from the data subject (e.g. the record of an interview with a parent). Article 14 applies where data about that data subject is obtained from *another* source (e.g. a social work report that includes information about that parent).

Safeguarders are responsible for the creation and content of their own PNs and guidance on this matter is available on the ICO website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Nevertheless, because of the unique role of the Safeguarder further guidance is provided below. It goes into rather a lot of detail but this is primarily to reassure Safeguarders that the lengthy provisions of the GDPR have been adequately considered and addressed in terms of the Safeguarder's role.

In this guidance the Safeguarders Panel Team has taken the view that Safeguarders should prioritise creating PNs with respect to Article 13 i.e. when obtaining data *directly* from the data subject. This is because the operation of Article 14(5)(c) of the GDPR means that providing the type of information required by Article 14 (i.e. in a PN) is not required when:

> *"obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests".*

'Obtaining or disclosure' of data by a Safeguarder is clearly subject to "Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests"

Consequently, the guidance in the table below concentrates on compliance with Article 13. However, it is for Safeguarders as data controllers to finally determine how they wish to approach the issue of information provision using a PN and the primary arbiter, in the UK, of what is and is not required of a Safeguarder under the GDPR is the ICO (the Court being the ultimate arbiter). Consequently, we have provided guidance with respect to Article 14 (also in tabular form) in the appendices (Appendix 2C) and Safeguarders can use it, if they wish, to create their own 'Article 14 PN'.

A PN should be as short, simple and jargon free as possible. It will typically be given in writing but it can be given orally, through signage or electronically.

A template for use with adults and older children and a template to use with younger children, both as derived from the second column below, are given at Appendix 2A and 2B. The ICO are in the process of producing an 'Age Appropriate Design Code' for communicating privacy information to children. While this is mainly for use with online services targeted at children, it may still be of use to Safeguarders.

| Article 13 (data from the data subject) | How this could be covered in a Safeguarder PN |
|---|---|
| 1(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; | Name & contact details of the Safeguarder |
| 1(b) the contact details of the data protection officer, where applicable; | N/A for Safeguarders |
| 1(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; | I am processing data (that is, information) about you and I am legally permitted to do this because I am a Safeguarder appointed to this case in accordance with Children's Hearings (Scotland) Act 2011. |
| 1(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; | N/A for Safeguarders |
| 1(e) the recipients or categories of recipients of the personal data, if any; | I am permitted to show this data to the following:<br>• Child/children<br>• Parents/carers/relatives<br>• 'Relevant persons' within the meaning of the Children's Hearings (Scotland) Act 2011<br>• Professionals involved (e.g. social workers, teachers, lawyers)<br>• The Hearing (i.e. panel members)<br>• The Court<br>• SCRA and its employees<br>• CHS and its employees<br>• The Safeguarders Panel Team (SPT) and its employees |
| 1(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. | N/A for Safeguarders |
| 2(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; | The data that I process shall be processed no sooner than from the date of my appointment and said processing will cease as soon as is practicable after the date of the occurrence of one or more of the termination |

| | |
|---|---|
| | events referred to in the Children's Hearings (Scotland) Act 2011 (Safeguarders: Further Provision) Regulations 2012 (No.336), at which point it will either be returned to the source from which it was obtained or be securely destroyed.<br><br>***A note on report sampling:***<br>If I am provided with a copy of any report *of which I am the author* for a purpose other than the use by me of said report in a case before the Children's Hearing or the Court I shall return that copy to the source from which it came or, if that is not possible, securely destroy that copy in all and any formats as soon as is practicable after the date at which the purpose for which the report was provided has been completely discharged.<br><br>In the particular case that I am provided with such a report by the Safeguarders Panel Team for the purposes of 'report sampling' as part of the Performance Support and Monitoring Framework applicable to me as a Safeguarder and as permitted by law; the date at which the purpose for which the report was provided has been completely discharged is normally the date no later than ten working days from the date of the meeting between me and the Safeguarders Panel Team at which the report was discussed.<br><br>Any retention of the report subsequent to the time period referred to above, without apparent justification, may be considered a data breach in terms of the data protection regime which the Safeguarders Panel Team may be obliged to report to the Information Commissioner's Office (ICO).<br><br>***A note on concerns:***<br>When I am provided with a copy of any material pertaining to a concern about me and which contains personal data I shall return that copy to the source from which it came or, if that is not possible, securely destroy that copy in all and any formats as soon as is practicable after the date at which the concern has been completely resolved.<br><br>The date at which the concern has been completely resolved is normally the date no later than ten working days after whichever of |

| | |
|---|---|
| | the following dates has most latterly occurred:<br>• The end of the period within which I may request a review of the outcome of a concern, that date being a date within twenty working days of the date on the 'concern outcome letter' as sent to the Safeguarder, without any such review being requested.<br>• When a review of the outcome of a concern having been requested has been completed, the date on the 'concern review outcome letter' as sent to me.<br><br>Any retention of the material subsequent to the time period referred to above, without apparent justification, may be considered a data breach in terms of the data protection regime, which the Safeguarders Panel Team may be obliged to report to the Information Commissioner's Office (ICO).<br><br>***A note on other processes:***<br>I may become subject to other processes (e.g. a police investigation) that are outwith my control. These will follow timescales of their own, which I cannot anticipate, and I will be obliged to process data in accordance with those processes and as advised by the people operating those processes or by the Information Commissioner's Office (ICO). |
| 2(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;<br><br>***NB please see note below the table*** | You have the right to see the data / information that I hold about you in a format that makes it easy for you to understand or pass on<br><br>You can ask me to<br>• change it<br>• destroy it<br>• only use it for certain purposes or not to use it at all<br><br>In most circumstances I will be able to do as you ask and I will be able to tell you what I have done. Sometimes I won't be able to do as you ask, for example, I need to use the data / information about you to do my safeguarding role in the way that the law says that I must. If this is the case I will let you know. |

| | |
|---|---|
| 2(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; | N/A for Safeguarders |
| 2(d) the right to lodge a concern with a supervisory authority; | You can make a concern about how I have used your data/information to the Information Commissioner's Office (ICO) www.ico.org.uk |
| 2(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; | N/A for Safeguarders.<br><br>(The fact is that no-one is obliged to speak to a Safeguarder except by virtue of their responsibilities to the Children's Hearings or the Court and a Safeguarder cannot compel them to nor can the Safeguarder compel anyone to provide him or her with documents). |
| 2(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. | N/A for Safeguarders |
| 3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. | N/A for Safeguarders (because they will never 'intend' to do so) |
| 4.Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information | In other words, if a Safeguarder knows that the data subject already knows all of the above information the Safeguarder doesn't need to give it to them all over again. |
| Exemptions | Depending on who you are, some people are allowed by law to make me show them the information that I hold about you.<br><br>If you are under sixteen or if a judge has put someone in place to help you deal with the important things in your life, then there are some people to whom, if they ask me to show them the information, I can sometimes say no. |

| | |
|---|---|
| | If you are under sixteen this would happen if the person who has asked me is a person who the law says is supposed to look after you.<br><br>If a judge has put someone in place to help you deal with the important things in your life this would happen if the person who has asked me is that person.<br><br>I can say no if giving them some kinds of information would mean telling them things about you that are not things that you would expect or want me to tell them or if giving them that information would be likely to cause you serious harm. |

***Note to the above re: Article 13(2)(b) and Article 14(2)(c) in Appendix 2C***

The further rights of a data subject and the rights of the data controller are set out at Articles 15 to 23. In terms of the text in the second column above, they can be referenced as follows:

You have the right to see the data / information that I hold about you (Article 15) in a format that makes it easy for you to understand or pass on (relates to Article 20)

You can ask me to:

- change it (relates to Article 16)
- destroy it (relates to Article 17)
- only use it for certain purposes or not to use it at all ((relates to Articles 18 and 21))

In most circumstances I will be able to do as you ask and I will be able to tell you what I have done. Sometimes I won't be able to do as you ask, for example, I need to use the data / information about you to do my safeguarding role in the way that the law says that I must. If this is the case I will let you know (related to Articles 19, 23).

Article 22 does not apply to Safeguarders because they do not do any automated processing.

In summary, Safeguarders should prioritise giving privacy notices to data subjects concerning the data subject's own data.

## 6. Data Retention and Destruction Policy

The approach to record keeping outlined above constitutes a data retention and destruction policy for Safeguarders i.e.

- The text set out re: Article 30(1)(f)): *"The data shall be processed no sooner than from the date of the Safeguarder's appointment and said processing will cease as soon as is practicable after the date of the occurrence of one or more of the termination events referred to in the Children's Hearings (Scotland) Act 2011 (Safeguarders: Further Provision) Regulations 2012 (No.336), at which point it will either be returned to the source from which it was obtained or be securely destroyed."*

- The notes above on:

    - Report sampling of the Safeguarder
    - Concerns about the Safeguarder
    - Other processes to which the Safeguarder becomes subject

- Practice Standard 5, particularly the part that reads: *"at the end of the Safeguarder's appointment, all information held by the Safeguarder in documentary or electronic format is returned as required or destroyed so that no information continues to be held unless the Safeguarder can justify this in line with policies and guidance relevant to Safeguarders".*

Data will therefore be retained for the periods outlined and not otherwise except when doing so can be justified in terms of other processes to which the Safeguarder becomes subject and which necessitates the possession of such personal data (e.g. a child protection concern, a police investigation).

If a Safeguarder is destroying data in the form of paperwork it should be shredded to ensure that it has been destroyed in a secure fashion. Putting papers into household waste or recycling is not acceptable as this is not a secure way to destroy paperwork.

When a Safeguarder tenders their resignation, all material pertaining to the role (including all paper or electronic files) must either be returned to the source from which it was obtained or be securely destroyed. Encrypted memory sticks must be returned to the Safeguarders Panel Team, having been cleared of all data. Safeguarders are also asked to check hard drives of any electronic devices used, including any mobile phones, used to ensure there are no materials on these systems. Safeguarders will be asked to confirm in writing that they have complied with this requirement.

In summary, Safeguarders should retain personal data for no longer than is necessary for the purpose for which such data is processed, whether that is the duration of a case (including any appeal period), the duration of the report sampling activity, the duration of a concern about them or the duration of other processes to which they become subject.

## 7. Data Breach

- *"A personal data breach means 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. It also means that a breach is more than just about losing personal data."* (ICO website)

The data controller must report a breach to the ICO *"not later than 72 hours after having become aware of it… unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"* (Article 33).

If *"the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay"* (Article 34).

Practice Standard 5 Confidentiality seeks to minimise the risk of breach. It states that

- *"a Safeguarder will maintain confidentiality and shall not disclose information unless in accordance with the law".*

If confidentiality is maintained then there is unlikely to be a data breach.

In practice, maintaining confidentiality includes the absolute necessity for Safeguarders to:

- type their own reports and all other communication and documentation
- not to allow anyone without a right to access that data, any access to that data, be that data electronic or physical

Practice Standard 5 also outlines the responsibilities of a Safeguarder to ensure that (amongst other things):

- *'the Safeguarders Panel Team and the Scottish Children's Reporter Administration are informed immediately when the Safeguarder has lost or mislaid information*
- *'appropriate action is taken if a Safeguarder is aware that there appears to be a breach of confidentiality due to another's action or inaction'.*

The responsibility for dealing with a data breach rests with the Safeguarder. However, the necessity for compliance with the Practice Standards for Safeguarders creates a locus for the SPT to be involved and the SPT is, in any case, available to assist Safeguarders in the event of a data breach. It is appreciated that breach may cause distress to a Safeguarder as well as to anyone whose data has been 'inappropriately processed', which in this context will typically mean that data has been lost or shared with / sent to someone with/to whom it should not have been shared/sent.

In the event of a data breach Safeguarders should, immediately upon becoming aware of the breach, contact and notify the following:

- the Safeguarders Panel Team
- the relevant Scottish Children's Reporter's Administration (SCRA) office
- the ICO (subject to the Article 33 criteria noted above)

Safeguarders should also be aware that the inappropriate sharing and disclosing of verbal information is also a data / confidentiality breach. Practice Standard 5, bullet point 4 explicitly states that:

- *"information is not disclosed in conversations in public places to others who have no right to know an individual's detail".*

If a data breach occurs despite a Safeguarder having complied with the Practice Standards for Safeguarders and their legal responsibilities under the GDPR, Safeguarders will receive support and guidance in reviewing their data management responsibilities and processes. Safeguarders will also be given help to put strategies in place to avoid a reoccurrence and to address the impact the data breach has on the child and any other person to whom the data breach relates to.

If a data breach occurs as a result of a Safeguarder's non-compliance with the Practice Standards for Safeguarders and/or their legal responsibilities under the GDPR Safeguarders must be aware that this will lead to careful consideration of their Ministerial appointment. In some cases breach could even result in potential prosecution under the relevant law.

In summary, compliance with the Practice Standards for Safeguarders will significantly reduce the risk of data breach but, usually, if a breach occurs it must be reported.

# 8. Data Storage and Transmission Including Use of Encrypted Memory Sticks

Closely allied to the issues of retention and breach is that of storage and transmission

As data controllers, Safeguarders will be responsible for the appropriate storage, transmission and destruction of the data in line with Practice Standard 5 which states that:

- *"information held electronically will be securely protected by him or her and in line with policies and guidance relevant to Safeguarders".*

Safeguarders must ensure that all information is protected and secured. In practice this means:

- Safeguarders have a responsibility to ensure that no other individual has access to any paper or electronic files and should be equally diligent in the workplace, at home or in transit;
- all electronic files (i.e. anything created, received and or otherwise generated during your role as a Safeguarder) must be stored on the secure encrypted memory stick only;
- no electronic data should ever be stored on the Safeguarder's home computer hard drive, the hard drive of the Safeguarder's work computer, or any other computer that the Safeguarder has access to; nor should any other form of portable electronic storage be used (i.e. an external hard disk, a memory card, a CD or DVD and so on). In practice this means as stated above, that all electronic data should be stored on the secure encrypted memory stick provided to, or authorised for use by, Safeguarders by the Scottish Government;
- the use of public cloud storage services, such as Google Docs, Amazon Cloud, Microsoft SkyDrive, DropBox and others, is not permitted;
- wherever and whenever possible, data should be stored electronically and not in paper form;
- when data is stored in paper form, all paper files should be kept in lockable storage to which only the Safeguarder has access.

Many of the requirements around data protection can be achieved through a common sense approach to data security, for example:

- if you leave any computer switched on and unattended, lock the computer;
- be conscious of who can see your work and screen, especially in public places;
- only print files if you are certain that you will collect the printing;
- never leave IT equipment unattended in public places and take special care in public places like airports, hotels and conferences or meetings;
- if you must leave IT equipment or any paperwork in your vehicle, ensure it is locked in the boot, out of sight;
- paperwork and computers should be transported in a locked carrier and no information should be visible to other travellers.

The Scottish Government has provided those Safeguarders who use Microsoft Windows software with an encrypted memory stick. Appendix 3 sets out practical guidance on how to operate the encrypted memory stick which is compatible with Windows software.

The Scottish Government ask that those Safeguarders who use Apple products purchase their own encrypted memory sticks. The make and model must be approved by the Scottish Government. Please see below a link to encrypted memory sticks provided by Apple and deemed acceptable by the Scottish Government. Safeguarders should decide which size of memory stick is most suitable for their use in the role of the Safeguarder and purchase the same. Safeguarders will then be reimbursed the cost of the memory stick (limited to a maximum of £20) by claiming this under the expenses section of the usual claim form and providing proof of purchase.

- Approved encrypted memory stick make and model: Integral 360 Secure USB 2.0 Flash Drive with 256-Bit Encryption Software. https://www.amazon.co.uk/d/USB-Flash-Drives/Integral-Secure-256-Bit-Encryption-Software/B007MCUCSO/ref=pd_sbs_147_5?_encoding=UTF8&psc=1&refRID=XSFJWHBCH71Y3HVG5C5N

Upon the cessation of a Safeguarder's appointment (for whatever reason), there is an obligation on the Safeguarder to return all encrypted memory sticks to the Safeguarders Panel Team within one month with written confirmation that the memory stick is clean of all data.

Safeguarders operating Apple software are asked to please contact Apple before accepting any software updates offered to ensure that the software update is compatible with the encrypted memory stick.

In summary, Safeguarders must store and transmit data securely and use only memory sticks either issued or approved by Scottish Ministers.

## 9. Electronic Transmission of Case Information – Use of Secure Email Such as CJSM

Emails or any other electronic communications that contain personal data are covered by the GDPR and the sixth of the revised principles relating to processing of personal data, the 'integrity and confidentiality' principle, as set out above, is especially relevant in this regard.

Email transmissions using standard email system (for example typical UK domestic email accounts such as Hotmail, TalkTalk, Gmail, Yahoo, Tiscali, BT Internet, Sky), if they can even be called secure at all, are certainly not sufficiently secure to ensure compliance with the GDPR as they can be highly susceptible to interception and interference. The vast majority of corporate email accounts will not be secure either.

Therefore if Safeguarders choose to use email in their practice, they must use an encrypted email system when sending personal data, whether that is in the body of the email or in attachments. Even very basic information such as the name of a child or family member, an address or a simple outline of the details of the case can count as personal data and so should be protected.

When communicating personal data to SCRA and the Safeguarders Panel Team by email, Safeguarders can use the Criminal Justice Secure Mail (CJSM) or any other secure mail system approved by the Scottish Government in the future for use by Safeguarders. Obviously the use of secure email is not required when no personal data is being communicated but Safeguarders need to be alert to situations involving email 'chains' where data which was initially sent securely may later be transmitted via unsecure networks, and also where data is not truly anonymised.

CJSM is a secure email system for transmission of data. It is currently used by SCRA and the Safeguarders Panel Team to send emails and information to Safeguarders about the cases that they are assigned to.

In order to be able to send and receive secure emails via CJSM, Safeguarders can obtain a CJSM email address free of charge. Practical guidance on setting up a CJSM email account is set out in a separate document. Please contact SPT for details.

Should SCRA change the secure email service that it uses, Safeguarders will be informed and provided with the necessary guidance.

It is the Safeguarder's responsibility to ensure that all email communication containing personal data is secure at all times.

When a Safeguarder tenders their resignation, they must deactivate any CJSM account set up solely for the purposes of their safeguarding role.

In summary, Safeguarders must use a secure email system, either CJSM or an equivalent.

## 10. Registering as a Data Controller

As made clear above, Safeguarders must register as 'data controllers' with the Information Commissioner's Office (ICO), which can be done online at this link https://ico.org.uk/for-organisations/register/

Appendix 5 provides a step-by-step guide to registering as a data controller with the ICO.

Data controller registration lasts for 12 months and must be renewed annually. The ICO will contact Safeguarders directly as regards the renewal of their registration.

The Scottish Government will reimburse the registration fee and all future renewal of registration fees. Safeguarders can claim back these fees as an expense (with proof of payment) on the national Safeguarders Panel expenses claim form.

Safeguarders are individually responsible for their own compliance with the GDPR. No responsibility for a Safeguarder's failure to comply with their responsibilities under the GDPR including as a data controller or obligation to ensure such compliance accrues to Scottish Ministers or to the Safeguarders Panel Team (SPT) irrespective of which legal or natural persons operate the SPT on behalf of Scottish Ministers.

In summary, Safeguarders must register as data controllers with the ICO and renew their registration annually.

## 11. Summary of What Safeguarders Have to do in Order to Comply With Their Legal Responsibilities Under the GDPR

1) Safeguarders will process personal data and special categories of personal data and must understand these terms and what forms 'data' can take.

2) Safeguarders must

   - only process personal data if they have a lawful basis to do so
   - process *all* 'personal data' in accordance with the seven principles
   - only process 'special categories of personal data' if they really need to in order to properly discharge their role and they if can pinpoint the legal basis (which will most likely be the public function or substantial public interest for special category personal data) which applies to that processing

3) Although strictly speaking Safeguarders may not require to produce a DPIA, as a matter of good practice, and to help protect themselves in the event of a data breach, Safeguarders should, nevertheless produce a *simple* DPIA. Conducting a DPIA, keeping a record of having done so and regularly reviewing it also helps to meet the seventh data protection principle ('accountability')

4) A Safeguarder must keep records of the type of personal data that they hold but only for the period for which they actually need to hold the personal data to which the records relate. After that period has ended the data must be securely destroyed immediately or within a certain timescale. Once it has been destroyed there is obviously no data held by the Safeguarder to which a record of the type of data held can relate. Consequently there is no need to keep a record of the type of data held unless it is actually *being* held. In any case, data may need to be made available to the ICO for inspection on request.

5) Safeguarders should prioritise giving privacy notices to data subjects concerning the data subject's own data.

6) Safeguarders should retain personal data for no longer than is necessary for the purpose for which such data is processed, whether that is the duration of a case (including any appeal period), the duration of the report sampling activity, the duration of a concern about them or the duration of other processes to which they become subject.

7) Compliance with the Practice Standards for Safeguarders will significantly reduce the risk of data breach but, usually, if a breach occurs it must be reported.

8) Safeguarders must store and transmit data securely and use only memory sticks either issued or approved by Scottish Ministers.

9) Safeguarders must use a secure email system, either CJSM or an equivalent.

10) Safeguarders must register as data controllers with the ICO and renew their registration annually.

## APPENDIX 1 – Practice Standard 5: Confidentiality

What:

- A Safeguarder will maintain confidentiality and shall not disclose information unless in accordance with the law.

Why:

- To respect peoples rights to privacy, in particular that of the child and family. To ensure that all Safeguarders treat information carefully and not share it beyond when this is allowed and required by law. To avoid breaching people's rights and causing distress to those affected by sharing information unlawfully, negligently or unintentionally.

How:

- It is the responsibility of a Safeguarder to ensure that:

  any documentation given to the Safeguarder in connection with a child by the reporter will be kept securely by the Safeguarder and returned to the reporter on termination of the Safeguarder's appointment information obtained by the Safeguarder will not be disclosed to others, except

  - as permitted by law
  - information about any crime that a child or other person indicates he or she will commit or, concerns about child protection or adult protection in line with the policies and guidance relevant to Safeguarders

- information held electronically will be securely protected by him or her and in line with policies and guidance relevant to Safeguarders

- information is not disclosed in conversations in public places to others who have no right to know an individual's details

- the Safeguarders Panel Team and the Scottish Children's Reporter Administration are informed immediately when the Safeguarder has lost or mislaid information

- at the end of the Safeguarder's appointment, all information held by the Safeguarder in documentary or electronic format is returned as required or destroyed so that no information continues to be held unless the Safeguarder can justify this in line with policies and guidance relevant to Safeguarders

- appropriate action is taken if a Safeguarder is aware that there appears to be a breach of confidentiality due to another's action or inaction.

## APPENDIX 2 – Privacy Notice Template

### A. A privacy notice template for use with adults and older children

My name is [name]. You can contact me at [contact details].

I am processing data (that is, information) about you and I am legally permitted to do this because I am a Safeguarder appointed to this case in accordance with Children's Hearings (Scotland) Act 2011.

I am permitted to show this data to the following:

- Child/children
- Parents/carers/relatives
- 'Relevant persons' within the meaning of the Children's Hearings (Scotland) Act 2011
- Professionals involved (e.g. social workers, teachers, lawyers)
- The Hearing (i.e. panel members)
- The Court
- SCRA and its employees
- CHS and its employees
- The Safeguarders Panel Team (SPT) and its employees

The data that I process shall be processed no sooner than from the date of my the appointment and no later than 24 hours after the date of the occurrence of one or more of the termination events referred to in the Children's Hearings (Scotland) Act 2011 (Safeguarders: Further Provision) Regulations 2012 (No.336), at which point it will be securely destroyed.

You have the right to see the data / information that I hold about you in a format that makes it easy for you to understand. You can ask me to

- change it
- destroy it
- only use it for certain purposes or not to use it at all

If I agree to what you ask I must tell you what I have done about it but I do not have to agree to what you ask. If I do not agree to do what you ask I have to explain my reason for not agreeing. Usually my reason will be that I need to use the data / information about you to do my safeguarding role in the way that the law says that I must.

You can make a complaint about how I have used your data/information to the Information Commissioner's Office (ICO) www.ico.org.uk

### B. A privacy notice template for use with younger children

My name is [name]. You can contact me at [contact details].

I collect information about you so that I can write a report about you for the Children's Hearing or the Court. I am allowed to do this because the law says so.

I am allowed to shoe the information that I have about you to:

- Child/children
- Parents/carers/relatives
- 'Relevant persons' within the meaning of the Children's Hearings (Scotland) Act 2011
- Professionals involved (e.g. social workers, teachers, lawyers)
- The Hearing (i.e. panel members)
- The Court
- SCRA and its employees
- CHS and its employees
- The Safeguarders Panel Team (SPT) and its employees

I only use that information for as long as your case lasts. After that I do not hold on to it.

You are allowed to see the information about you that I have. I have to make sure I give it to you in way that you can understand. can ask me to

- change it
- destroy it
- use it for one thing and not for another.

If I agree to what you ask I must tell you what I have done about it but I do not have to agree to what you ask. If I do not agree to do what you ask I have to explain my reason for not agreeing. Usually my reason will be that I need to use the data / information about you to do my safeguarding role in the way that the law says that I must.

You can make a complaint about how I have used your information to the Information Commissioner's Office (ICO) www.ico.org.uk

### C. Article 14 Privacy Notice

| Article 14 (data from another source) | How this could be covered in a Safeguarder PN |
|---|---|
| 1(a) the identity and the contact details of the controller and, where applicable, of the controller's representative; | Same as Article 13 |
| 1(b) the contact details of the data protection officer, where applicable; | N/A for Safeguarders |
| 1(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; | Same as Article 13 |
| 1(d) the categories of personal data concerned; | Categories of personal data:<br>• Name and contact details<br>• Description of prior and present actions and views in relation to the matters with which the case at hand is concerned and supporting details as set out in the Safeguarder's report or reports to the Hearing or Court<br>• Reports from third parties (e.g. social work) |
| 1(e) the recipients or categories of recipients of the personal data, if any; | • Child/children<br>• Parents/carers/relatives<br>• 'Relevant persons' within the meaning of the Children's Hearings (Scotland) Act 2011<br>• Professionals involved (e.g. social workers, teachers, lawyers)<br>• The Hearing (i.e. panel members)<br>• The Court<br>• SCRA and its employees<br>• CHS and its employees<br>• The Safeguarders Panel Team (SPT) and its employees |
| 1(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available; | N/A for Safeguarders |
| 2(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; | Same as Article 13 |

| | |
|---|---|
| 2(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; | Same as Article 13 |
| 2(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; | Same as Article 13 |
| 2(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; | N/A for Safeguarders |
| 2(e) the right to lodge a complaint with a supervisory authority; | Same as Article 13 |
| 2(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; | This will vary from case to case but is likely to mainly consist of:<br>• interviews with other people involved in the case<br>• reports by professionals (e.g. social work) |
| 2(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; | N/A for Safeguarders |
| 3.The controller shall provide the information referred to in paragraphs 1 and 2… | - |
| (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; | In other words, for each piece of data obtained by the Safeguarder the Article 14 information should be provided to the data subject within one month of the Safeguarder having obtained that piece of data<br><br>This is clearly impractical. Safeguarders should stick to providing any Article 14 information that may be required at the beginning of the case. |
| (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or | In other words, data to be used for contacting Article 14 information, insofar as it pertains to the data subject's contact details, must be provided to the data subject at the point of first contact. |

| | |
|---|---|
| (c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed | In other words, if you share data obtained from a source other than the data subject with anyone else, you should let the data subject know this at the point of first sharing.<br><br>This is clearly impractical. Safeguarders should stick to providing any Article 14 information that may be required at the beginning of the case. 'Recipients' should all fall within the categories noted above. |
| 4.Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2. | N/A for Safeguarders |
| 5.Paragraphs 1 to 4 shall not apply where and insofar as: | This means "none of Article 14 so far will apply if one or more of the following applies" |
| (a) the data subject already has the information; | Same as Article 13. |
| (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; | N/A for Safeguarders.<br><br>It is almost inconceivable that it would prove impossible or would require disproportionate effort for a Safeguarder to provide the information concerned nor is it likely to 'render impossible or seriously impair the achievement of the objectives of that processing' as the Safeguarder's primary sources of information about a data subject other than the data subject him/herself are professionals whose reports are available to the data subject anyway. Insofar as such data may constitute the 'testimony' of others *and* the Safeguarder is of the view that providing it may 'render impossible or seriously impair the achievement of the objectives of that processing' the Safeguarder can base a refusal on this section and, if the person requesting the data wishes to complain about that position, the Safeguarder can refer that person to the ICO. |
| (c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; | It is the Safeguarders Panel Team's interpretation of Article 14(5)(c) that Safeguarders should not need to give a PN to those people who fall under Article 14 |

| | |
|---|---|
| (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy. | This may apply in the circumstances of a particular case but it is unlikely to apply as a matter of course. |

## APPENDIX 3 – How to Use a Memory Stick That is Compatible With Microsoft Windows Software

SDMS encrypted flash memory device operating instructions

On first use:

1. Insert the encrypted memory stick into the computer and open “my computer”. You will see a new “CD/DVD drive” and a new “hard disk drive”.

2. Double click on the CD/DVD drive and then double click on the icon “Lock233_8ch”

3. You will be prompted to put in your password. This has to be a minimum of 8 characters. It must contain at least one alpha character, one numerical character and one special character (! ” £ etc.).

4. Tab to the next section and type your password in again.

5. Tab to the next section and type in a hint. You will not be able to use the password as your hint.

6. You will now be presented with a new screen.

7. Click on the “padlock” icon.

8. Type in your password and click on the “tick” icon.

9. If you have used the correct password you will see a message “Secure Drive is Now Accessible”.

10. To access the “secure drive” which may now be called “AES_Disk” you need to open “My Computer” and double click on the relevant drive.

11. If you put the password in incorrectly 10 times the device will be locked.

12. To unlock the device it will need to run on a computer on which the operator has Administrator privileges.

13. Once unlocked start at instruction 1.

## APPENDIX 4 – How to Register as a Data Controller With ICO

- Google ICO or follow this link: https://ico.org.uk/
- Click on “Pay fee, renew fee or change your details” on the right hand side of the screen
- Having read the page, please click on “Register” then “start new registration application”
- There then will appear a series of questions. Below we have detailed the questions asked and the responses Safeguarders should put:-

**Section 1 - About you**

| **Question** | **Response and any comment** |
|---|---|
| Organisation type | Other |
| Please give details | Safeguarder |
| Organisation name | Insert Safeguarder’s name |
| Address | **Please note that this address will appear on the ICO’s public register so Safeguarders may wish to put a c/o address**. Should Safeguarders want to, they may use the address of the Safeguarders Panel Team which is:-<br><br>Children 1st<br>83 Whitehouse Loan<br>Edinburgh<br>EH9 1AT<br><br>Should Safeguarders wish to change the address entered at any time in the future, they simply have to email ICO or telephone the ICO helpline on 0303 123 1113 (local rate) or 01625 545 745 (national rate) |
| Your organisation may already beregistered. Is your organisation one of the following? | No, I'm registering for the first time (continue with registration) |
| Trading names | Leave blank |
| Are you a public authority? | No |
| ***Fee calculator*** | |
| Is your organisation a charity or have exempt charitable status? | No |
| Is your organisation a small occupational pension scheme | No |
| Does your organisation have 10 members of staff or fewer? | Yes |
| Main contact details. Please enter the details of the person who is | Please add **your** details. These will NOT be made public and will be used only by the ICO to enable them to contact the |

| | |
|---|---|
| responsible for the registration | Safeguarder in relation to their registration and any subsequent re-registrations. Please, if possible, provide an email address as email is the ICO's preferred method of contact. |
| ***Does your organisation need a data protection officer (DPO)?*** | |
| Do your organisation's core activities involve tracking and monitoring people's behaviour (for example on the internet or on CCTV) on a large scale? | No |
| Do your organisation's core activities involve processing on a large scale "special categories" of personal data, or large scale criminal convictions or offences data? | No (unless the Safeguarder particularly wishes to say Yes, which they are free to do, see further details below).<br><br>"Special categories" means personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs or trade unions membership, data concerning health or data about a person's sex life or sexual orientation, or genetic or biometric data where it would identify a living person.<br>Should Safeguarders consider that they process on a large scale "special categories" of personal data, or large scale criminal convictions or offences data, then the answer is yes and then they should provide their own contact details. It is suggested that Safeguarders do not tick the box next to "Publish name on the public register".<br>Should Safeguarders consider that they do not process on a large scale "special categories" of personal data, or large scale criminal convictions or offences data, then the answer is no.<br>This will mean that it is not deemed necessary for the Safeguarder to nominate a DPO, however, the Safeguarder can chose to nominate one (themselves) on a voluntary basis or provide a contact for data protection (themselves). Please note that if a Safeguarder choses to nominate a DPO, their contact details *will* be published on the public register. Should Safeguarders chose to provide a contact for data protection, the Safeguarder can *chose* whether their contact details are published. |
| Your organisation does not need a data protection officer. However, you can nominate one, or provide a contact for data protection in your organisation. | No thanks (unless you have responded Yes to the previous question or you actually want to nominate a data protection officer, in which case your subsequent answers will be for you to determine) |
| Person completing this form | Tick the box next to "Use details from 'Main contact details' above" |

* This enables the annual fee of £40 to be calculated. Please note that this will be reimbursed to Safeguarders by the Scottish Government upon submission of proof of payment to the Safeguarders Panel Team using the national Safeguarders Panel expenses claim form.

When making payment, Safeguarders are recommended to select the option to set up annual direct debit payment which will reduce the cost to £35.

**Click on Next>>**

**Section 2- Registration details**

| Question | Response and any comment |
|---|---|
| Nature of work | Scottish Safeguarder |

**Tick to confirm Declaration >>**

**Click on Next>>**

- There then follows a confirmation screen summarising the information inputted with a declaration at the bottom of it.

- Finally, payment is required. As mentioned above, the registration fee will be reimbursed to Safeguarders by the Scottish Government upon submission of proof of payment to the Safeguarders Panel Team using the national Safeguarders Panel expenses claim form.