Helping Hands

WORK INSTRUCTION (WI)

Title of WI	Data Incident Risk Management		
What type of document is this?	Work Instruction	**WI Reference Number**	HHH-W.I-004
Purpose of WI	This working instruction is to be used in conjunction with the Helping Hands Data Incident procedures to ensure that incident detection, investigation, internal reporting and notification where applicable, takes place. This document facilitates risk assessment and notification process.		
Role	Responsibility		
Data Protection Officer (DPO)	Responsible for providing advice on handling data incidents, risk management and data breach notification to the ICO.		
GDPR Coordinator	The GDPR Coordinator is responsible for monitoring the data incident inbox and liaising with the relevant employees and the DPO on incident risk management.		
All Employees	To adhere to this work instruction where applicable.		
Scope of WI	This work instruction applies to Helping Hands GDPR Coordinator, Data Protection Officer and Quality. The GDPR Coordinator will liaise with relevant employees regarding instructions on incident risk management.		

1.0 Risk Assessment Grid and Score Rationale

1.1 Risk Rating Key:

Extreme – Consultation with DPO required, DPO report to ICO, Executive team,	High – Notification to affected Individuals,	Moderate – Notification to affected individuals,	Low – Notification to affected individuals

Board and affected individuals	Consultation with DPO required	consultation with DPO on a case-by-case basis	

1.2 Risk Assessment Grid

Likelihood that individuals have been affected (harm)					
Almost Certain	Moderate	High	Extreme	Extreme	Extreme
Likely	Low	Moderate	High	Extreme	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Low	Moderate	Moderate	High
Rare	Low	Low	Low	Low	Moderate
	Negligible	Minor	Moderate	Major	Severe
	Impact (severity)				

Step 1: Likelihood of affecting individuals

Likelihood	Description
Rare	Isolated incident. No evidence to support that harm has occurred. Not a frequent or regular occurrence. No lasting effect is anticipated

Unlikely	Isolated incident unlikely to reoccur. No evidence to support that harm has occurred. Not a frequent or regular occurrence. No lasting effect is anticipated
Possible	Potential to occur frequently and regularly and possibly affect individual
Likely	Likely to occur frequently and regularly and likely to affect individual
Almost Certain	Recurring and frequent, predictable patterns, almost certain to affect individual

Step 2: Impact of the Incident

Severity	Description
Negligible	• No risk to individual rights and freedoms resulting from the incident • Minimal effect and/or risk of harm to affected individuals. • Data containment measures in place at time of incident* • Minimal exposure at unsecured location • No risk of confidential information leading to embarrassment • No risk of litigation, ID fraud, loss of funds or employment
Minor	• Minor risk to individual rights and freedoms resulting from the incident • Minor effect and/or risk of harm to affect individuals • Data containment measures in place at time of incident* • Minimal exposure at unsecured location • Low risk of confidential information leading to embarrassment • Low risk of litigation, ID fraud, loss of funds or employment
Moderate	• Due care/process below reasonable expectations in several ways, but not for prolonged periods. • Has potential to impact on service provision and /or affects vulnerable individuals. • Requires investigation relating to compliance and risk

	management issues. • Some potential for litigation and adverse local publicity
Major	• Due care/process below reasonable expectations in several ways which may have a lasting effect • Likely to impact on service provision and /or affects vulnerable individuals. • Requires investigation relating to compliance and risk management issues. • Likely for litigation and adverse local publicity
Severe	• Significant issues regarding standards, quality of care, and safeguarding of, or breach of rights and freedoms. • Compliance and risk-management issues causing long term issues for those affected. • Loss of control of personal data, unauthorised reversal of anonymization /pseudonymisation • High probability of loss of employment, financial loss and/or fraud • Excessive and disproportionate volume affected by incident. • Will require immediate and in-depth investigation due to the potential risk of embarrassment and/or discrimination • May involve serious safety issues, reputational damage and/or strong possibility of adverse national publicity. • A high probability of litigation, financial loss, decline in health and/or death

2.0 Data Containment Measures

There are circumstances where containment action will negate the need to notify the ICO of a breach of personal data.

- encryption – where the personal data is protected by means of encryption.
- 'trusted' partner - where there may be a confidentiality or availability incident whereby personal data is accidentally sent or disclosed the wrong department or a regular contractor known to Helping Hands. In such situations, the data may be recovered,

  returned or securely destroyed. The recipient may still be considered "trusted" even if the data has been accessed if Helping Hands can be assured that the data has not been further compromised.
- cancel the effect of a incident - where the controller can null the effect of any personal data incident

Helping Hands acknowledges that such cases will need to be reported and risk assessed

following a incident. This in turn may reduce the risk to individuals warranting a 'near event'

classification and rendering notification to ICO unnecessary;

2.1 Sensitivity Factors

Certain factors need to be considered and incorporated in to the grading scores. When a incident involves special category data and/or vulnerable groups, this will increase the risk score and may

lead to notification to affected individuals and ICO being a higher priority.

2.2 Vulnerable Groups

- Children and vulnerable young people
- Vulnerable adults with Safeguarding concerns

2.3 Special Categories of personal data

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- processing of genetic data,
- biometric data for uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation

2.4 Other data not listed under GDPR

- Criminal convictions/prisoner information
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health

3.0 Notification Procedure

Article 34 of GDPR requires that any personal data incident resulting in a high risk of harm/impact to the rights and freedoms of individuals needs to be communicated with those affected with the following notable exceptions:

The controller (Helping Hands) has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the incident; for example, the data were encrypted.

The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms if individuals is no longer likely to materialise.

It would involve a disproportionate effort. However, there is still an obligation to have a communication by another means such as a press notice or statement on the organisation website.

The article outlines that a data incident with a significant risk score as indicated in the risk rating key needs to be reported to the relevant authority who are the ICO.

The following information is to be included in any notification in both circumstances and shown below:

- A description of the nature of the personal data incident, data category and approximate number of data subjects and volume of records where possible
- Name and contact details of the DPO or other contact from whom more information can be obtained

- Description of the likely consequences of the incident and
- Description of the measures taken or proposed to address the incident, including any measures to mitigate possible adverse effects.

Article 33 of GDPR requires reporting of a incident within 72 hours. This period starts when Helping Hands becomes aware of the incident and not necessarily when the incident occurred. There must be an established process to determine that a security incident has occurred which has led to personal data being compromised.

Don't delay in reporting an incident if you are unsure on whether to report– if in doubt err on the side of caution and notify.

Don't put anything in the report that could be considered personal confidential data (such as patients / service user details)

If the decision is made not to notify individuals, there may still be a need to notify the ICO unless Helping Hands can demonstrate that the incident is unlikely to result in a risk to rights and freedoms. The ICO has the power to compel organisations to inform affected individuals if it considers there is a high risk.

There must be clear documentation of any decision-making process in line with the requirements of this SOP.

Where the 72hour deadline is not met, an explanation must be provided to the authorities as failure to notify promptly may result in additional action by the ICO in respect to GDPR.

3.1 What to expect following notification

An email from the ICO will be sent to confirm receipt of the notification and an ICO case reference number which must be noted and quoted in any further correspondence with the ICO in relation to the incident.

3.2 Records

All documentation, records and information pertaining to a incident must be logged, maintained and made available on request. The current location is:

- *SharePoint / Home / Record Keeping/ Data Incident Log*
- *SharePoint / Documents / GDPR Compliance/ Data Incident/ DIN Forms*

The Information Commissioner will then decide if any action is necessary and whether other authorities need to be notified and to what extent.

TRAINING Is training required?	No
COMPLIANCE	Compliance will be monitored via the GDPR Coordinator and the Information Governance Steering Group

How is compliance with this document going to be monitored?		
PROCEDURAL INFORMATION		
Changes since previous version	Review of section 1.0 - Risk Management Grid and rationale. Aligned with data incident notification form. Revised the terminology for 'data breaches' to 'data incidents' - updated onto new template	
Who was involved in developing /reviewing/amending the document? (list titles)	GDPR Co-Ordinator Data Protection Officer Quality Development Lead	
How confidential is this document	Restricted	Can be shared freely within Helping Hands but NOT outside
References		
Associated Documents	*Data Protection Policy* *Data Incident Notification (DIN) Form*	