PERSONAL DATA BREACH POLICY

At No Going Back, we take the protection of personal data and privacy very seriously. This data breach policy should be followed when a data breach arises and sets out the process to be followed in order to ensure that the appropriate action is taken to reduce the impact of the data breach on our customers and ensure the reporting and recording requirements as set out in data protection legislation are completed.

1 Introduction

1.1 This personal data breach policy:

1.1.1 places obligations on staff to report actual or suspected personal data breaches; and

1.1.2 sets out our procedure for managing and recording actual or suspected breaches.

1.2 This policy applies to all staff, and to all personal data and special category personal data held by No Going Back. This policy supplements our policies relating to data protection, information security and list any other relevant policies.

1.3 The table below explains some key terminology used in this policy:

Term	Meaning
Personal data breach	A breach of data security leading to the: - accidental or unlawful destruction; - loss; - alteration; - unauthorised disclosure; or

Term	Meaning
	- access to personal data transmitted, stored, or otherwise processed—e.g. accidental loss, destruction, theft, corruption, or unauthorised disclosure of personal data.
Personal data	Information relating to a living individual who can be identified (directly or indirectly) from that information.
Data subject	The individual to whom the personal data relates.
Special category personal data (sometimes known as sensitive personal data)	Personal data revealing racial or ethnic origin, political opinions, religious beliefs, philosophical beliefs or trade union membership, genetic data biometric data (where used for identification purposes), data concerning health, sex life or sexual orientation
Information Commissioner's Office (ICO)	The UK's independent data protection regulator

2 Responsibility

Our internal data manager has overall responsibility for this policy. They are responsible for ensuring it is complied with by all staff.

3 Our duties

3.1 No Going Back processes personal data relating to individuals including staff, clients and third parties. As custodians of data, we have a responsibility under UK data protection law to protect the security of the personal data we hold.

3.2 We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies (in particular our Data Protection Policy).

4 What can cause a personal data breach?

4.1 A personal data breach can happen for a number of reasons:

4.1.1 loss or theft of data or equipment on which data is stored, e.g. loss of a laptop or a paper file;

4.1.2 inappropriate access controls allowing unauthorised use;

4.1.3 equipment failure;

4.1.4 human error, e.g. sending an email to the wrong recipient;

4.1.5 unforeseen circumstances such as a fire or flood;

4.1.6 hacking, phishing, and other 'blagging' attacks where information is obtained by deceiving whoever holds it;

4.1.7 alteration of personal data without permission; and

4.1.8 loss of availability of personal data.

5 If you discover a personal data breach

5.1 If you know or suspect a personal data breach has occurred or may occur, you should:

5.1.1 complete a data breach report form, which can be found at Appendix 1; and

5.1.2 email the completed form to stuart@nogoingback.org.uk.

5.2 Where appropriate, you should liaise with your line manager about completion of the data breach report form. However, this may not be appropriate or possible, e.g. if your line manager is aware of the breach and has instructed you not to report it, or if they are simply not available. In these circumstances, you should submit the report directly to stuart@nogoingback.org.uk without consulting your line manager.

5.3 You should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators.

6 Managing and recording the breach

6.1 On notification of a data breach, we will take appropriate action to:

6.1.1 contain the data breach and (so far as reasonably practicable) recover, rectify, or delete the data that has been lost, damaged, or disclosed;

6.1.2 assess and record the breach in No Going Back' data breach register;

6.1.3 notify appropriate parties of the breach; and

6.1.4 take steps to prevent future breaches.

These are explained below.

6.2 Containment and recovery

6.2.1 We will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of personal data.

6.2.2 We will identify ways to recover, correct or delete data. This may include contacting the police, e.g. where the breach involves stolen hardware or data.

6.2.3 Depending on the nature of the breach, we will notify our professional indemnity insurer, cyber insurer and/or crime insurer. We will decide if

it is appropriate to engage the insurer's data breach management experts.

6.3 Assess and record the breach

6.3.1 Having dealt with containment and recovery (see section 6.2), we will assess the risks associated with the breach, including:

(a) what type of data is involved?

(b) how sensitive is the data?

(c) who is affected by the breach?

(d) the likely consequences of the breach on affected data subjects?

(e) where data has been lost or stolen, are there any protections in place such as encryption or pseudonymisation?

(f) what has happened to the data, e.g. if data has been stolen, could it be used for harmful purposes?

(g) what could the data tell a third party about the data subject?

(h) what are the likely consequences of the personal data breach on ?

(i) are there wider consequences to consider, e.g. loss of public confidence in an important service we provide?

6.3.2 Details of the breach will be recorded in No Going Back' data breach register.

6.4 Notifying appropriate parties of the breach

6.4.1 We will consider whether to notify:

(a) the ICO (see 6.5.2 below);

(b) affected data subjects (see 6.5.3 below);

(c) the police (see 6.5.4 below);

(d) Office of the Immigration Services Commissioner (OISC) (see 6.5.5 below); and/or

(e) any other parties, e.g. insurers or commercial partners.

6.4.2 Notifying the ICO

(a) We will notify the ICO when a personal data breach has occurred unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects.

(b) Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after we became aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay.

(c) If we are unsure whether to report, the presumption should be to report. We will take account of the factors set out below:

1	The potential harm to the rights and freedoms of data subjects
2	This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include: — exposure to identity theft through the release of non-public identifiers, e.g. passport number; — information about the private aspects of a person's life becoming known to others, e.g. financial circumstances. The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

3	The volume of personal data
4	There should be a presumption to report to the ICO where: — a large volume of personal data is concerned; and — there is a real risk of individuals suffering some harm. It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances of the loss or the extent of information about each individual.
5	The sensitivity of data
6	There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress. This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples: — theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable; breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

6.4.3 Notifying data subjects

(a) Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, We will notify the affected data subject(s) without undue delay, including:

(i) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(ii) the likely consequences of the personal data breach; and

(iii) the measures we have or intend to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

(b) When determining whether and how to notify data subjects of the breach, we will:

(i) co-operate closely with the ICO and other relevant authorities, e.g. Office of the Immigration Services Commissioner (OISC) and/or the police

(ii) take account of the factors set out in the table below:

Factor	Subject
Whether we have implemented and applied (to the affected personal data) appropriate technical and organisational protection measures—in particular measures that render the personal data unintelligible to	Where such measures have been implemented, it is not necessary to notify the data subject(s).

any person who is not authorised to access it, e.g. encryption.	
Whether we have taken measures following the personal data breach which ensure the high risk to the rights and freedoms of data subjects affected by that breach is no longer likely to materialise.	Where such measures have been implemented, it is not necessary to notify the data subject(s).
Whether it would involve disproportionate effort to notify the data subject(s).	If so, it is not necessary to notify the data subject(s) individually —but we must, instead, issue a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
Whether there are any legal or contractual requirements to notify the data subject?	If yes, it may be necessary to notify the data subject(s) in any event.

6.4.4 Notifying the police

We will already have considered whether to contact the police for the purpose of containment and recovery (see section 6.2). Regardless of this, if it subsequently transpires that the breach arose from a criminal act, we will notify the police and/or relevant law enforcement authorities.

6.4.5 Notifying other parties

We will consider whether it is appropriate to notify the Office of the Immigration Services Commissioner (OISC), or if there are any legal or contractual requirements to notify any other parties.

6.5 Preventing future breaches

Once the personal data breach has been dealt with, in accordance with this policy, we will:

6.5.1 establish what security measures were in place when the breach occurred;

6.5.2 assess whether technical or organisational measures can be implemented to prevent the breach happening again;

6.5.3 consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;

6.5.4 consider whether it is necessary to conduct a privacy risk assessment; and

6.5.5 update our privacy risk register.

7 Monitoring and review

7.1 We will monitor the effectiveness of all our policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.

7.2 Our monitoring and review exercises will include looking at how our policies and procedures are working in practice to reduce the risks posed to our company.

8 Staff awareness and training

8.1 Key to the success of our systems is staff awareness and understanding.

8.2 We provide regular training to staff:

8.2.1 at induction;

8.2.2 when there is any change to the law, regulation, or our policy;

8.2.3 when significant new threats are identified; and

8.2.4 in the event of an incident affecting our company or a competitor.

9 Reporting concerns

9.1 Prevention is always better than cure.

9.2 Data security concerns may arise at any time, and we encourage you to report any concerns you have to stuart@nogoing back.org.uk. This helps us capture risks as they emerge, protect our company from personal data breaches and keep our processes up-to-date and effective.

10 Consequences of non-compliance

10.1 Failure to comply with this policy and associated policies on data protection puts you and No Going Back at risk. Failure to notify stuart@nogoingback.org.uk of an actual or suspected personal data breach is a very serious issue.

10.2 You may be liable to disciplinary action if you fail to comply with the provisions of this, and all related plans, policies, and procedures.

APPENDIX 1

DATA BREACH REPORT FORM

If you know or suspect a personal data breach has occurred, please:

- complete this form, and
- email it to stuart@nogoingback.org.uk, ensuring you mark your email or the form as urgent.

Name and contact details of person notifying the actual or suspected breach	*Insert name and contact details*
Dept/manager	*Insert department from which the report emanated and the relevant manager*
Date of actual or suspected breach	*Insert date*
Date of discovery of actual or suspected breach	*Insert date*
Date of this report	*Insert date*
Summary of the facts	*Provide as much information as possible including the amount, sensitivity and type of data involved*
Cause of the actual or suspected breach	*Provide a detailed account of what happened*

Is the actual or suspected breach ongoing?	☐ Yes ☐ No ☐ Not known
Who is or could be affected by the actual or suspected breach?	*Include details of categories and approximate number of data subjects concerned. Do not notify the data subjects as we will determine if this is appropriate.*
Are you aware of any related or other data breaches?	☐ Yes ☐ No *If yes, provide more details*