Peak District National Park Authority
Data Breach Process

September 2020

Version	Author	Approved By	Approval Date	Publication Date	Review Date
1.0	**MS**	**Head of Information Management**	**18/05/2018**	**18/05/2018**	**18/05/2019**
1.1	**MS**			**11/09/2020**	**11/09/2021**

Introduction

The General Data Protection Regulation (GDPR) introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority, which in the UK is the Information Commissioner (ICO).

Contents

Purpose

By implementing this procedure we will ensure that there is a consistent approach to the way in which we record, evaluate, report and respond to data protection breaches. In particular it will help us to identify and facilitate improvement when required and thus reduce the likelihood of recurrence, and help to support individuals whose personal data may have been compromised.

Scope and Responsibilities

The procedure applies to:

- All personal data that we process, across all our locations and regardless of format;
- All staff as referenced in the Introduction, who have access to and use the information;
- All third parties as referenced in the Introduction who have access to the information and may be responsible for processing the information on our behalf;

Types of Data Protection Breaches

These can include:

- Misdirection of emails or correspondence concerning personal data;
- Loss or theft of papers containing personal data;
- Personal data received in error;
- Unauthorised publication of personal data on website;
- Loss or theft of data storage devices containing personal data; such as laptop, memory stick, tablet or smart phone.

Reporting a Breach

A data protection breach should be reported as quickly as possible after discovery, Contact the Head of Information Management, or in his absence, the Data Manager and DPO.

Once reported, the breach will be logged and assessed, with initial advice provided as required, including taking remedial action as necessary.

Response and Containment

To determine the appropriate level of response and further actions, service areas may be asked to provide further details. Heads of Service are expected to co-operate fully and respond promptly.

The following steps should be taken:

- Establish who should be made aware of the breach;

- Identify and implement any steps required to contain the breach – this might involve requesting the return correspondence sent in error or to the wrong recipient;
- Identify and implement any steps required to recover any losses and limit the damage of the breach;
- It might be necessary to inform appropriate bodies or regulators such as the ICO, the police or an insurance company.

Assessment of Risk

Any breach must be managed according to its risk. Following containment of the breach, the risks should be assessed in order to identify an appropriate response. The checklist in **Appendix A** should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

Informing the Individual(s)

Consideration will need to be given as to whether the individual(s) should be notified of the breach. This will depend on the nature of the breach and should be carefully managed. Factors to consider include:

- The sensitivity of the information;
- Volume of information;
- Likelihood of unauthorised use;
- Impact on the individual(s) concerned;
- Ease of contacting the individual(s)

Don't be too quick to disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete and serves a purpose.

It might be appropriate to involve the Communications Team who will be able to offer advice on the content of any message or press release. It is important that we are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated properly.

Consideration should be given to the following:

- Details of what happened and when the breach occurred;
- The data involved;
- Steps taken to contain the breach and prevent reoccurrence;
- Advice on steps they should take, such as contacting banks;
- Any assistance we can offer and if necessary, how we will keep them informed;

- Provide a point of contact.

It might be necessary to inform appropriate bodies or regulators such as the ICO, the police or insurers.

Notifying the Information Commissioner

In addition to notifying individual(s) or other parties, consideration will have to be given to notifying the ICO; the regulatory body with responsibility for promoting and enforcing data protection legislation.

Where there is an identified risk to the individual(s), for example the breach is likely to result in some degree of damage and/or distress, we will be required to notify the ICO within 72 hours of discovering the breach.

Evaluation and Recommendations

Regardless of the type and severity of the incident, all breaches need to be fully assessed to identify if improvement actions are required. While some breaches may not require further action (some will be false alarms or near misses), it is likely that a number of measures may need to be implemented to reduce the risk of it happening again. These may include:

- Reinforcing existing procedures and raising awareness;
- Revising procedures for processing personal data;
- Refresher training for staff;
- Introducing enhanced security arrangements for personal data.

We must be able to demonstrate that measures have either been put in place or there is a documented plan to do so. This has been a recurrent theme of ICO enforcement and it's important that our procedures reflect this.

Appendix A: Security Breach Assessment Checklist

a) What is the nature of the breach? Please provide as much detail as possible, including what happened, for example loss of laptop containing personal data, email containing personal data sent to wrong recipient

b) How did the breach occur?

c) What type of data is involved, for example, mobile number, medical records etc.?

d) How many individuals are affected?

e) Who are the individuals, for example, employees, customers etc.?

f) What has happened to the data?

g) Establish a timeline
   a. When did the breach occur?
   b. When was it discovered?
   c. When was it contained?

h) Was there any protection in place, for example, the data was encrypted, file was password protected?

i) What are the potential consequences for us:
   a. Level of severity?
   b. How likely are they to occur?

j) What could the data tell a third party about an individual
   a. What harm could this cause, for example financial loss, emotional damage etc.?

k) Does the information have a commercial value that could be exploited, perhaps as part of a criminal activity?

Appendix B Data Protection breach notification form

1.	**Organisation Details**
	a)* What is the name of the organisation – is it the data controller in respect of this breach
	b) Please provide the data controller's registration number – if applicable
	c)* Please provide details of your DPO
2.	**Details of the data protection breach**
	a)* Please describe the incident in as much detail as possible
	b)* When did the breach happen
	c)* How did the incident happen
	d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.
	e) What measures did the organisation have in place to prevent an incident of this nature occurring?
	f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.
3.	**Personal data placed at risk**
	a)* What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent
	b)* How many individuals have been affected?
	c)* Are the affected individuals aware that the incident has occurred?
	d)* What are the potential consequences and adverse effects on those individuals?
	e) Have any affected individuals complained to the organisation about the incident?
4.	**Containment and recovery**
	a)* Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so , please provide details.
	b)* Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
	c) What steps has your organisation taken to prevent a recurrence of this incident?
5.	**Training and guidance**
	a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act. If so, please provide any extracts relevant to this incident.
	b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?
	c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident which you are reporting. If so, please provide any extracts relevant to this incident here.
6.	**Previous contact with the ICO**
	a) * Have you reported any previous incidents to the ICO in the last two years?
	b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported, where known, the ICO reference number.
7.	**Miscellaneous – if applicable**

	a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.
	b) Have you informed the Police about this incident? If so, please provide details.
	c) Have you informed any other regulatory bodies about this incident? If so, please provide details.
	d) Has there been any media coverage of this incident? If so, please provide details of this.