

Personal Data Breach Policy

**CONTENTS**

 **Page**

1. Introduction 3
2. Purpose 3
3. Roles and Responsibilities 3
4. Ensuring Breaches Do Not Happen 4
5. What is a Personal Data Breach 4
6. Types of Personal Data Breaches 5
7. Dealing with a Breach 5
8. Notifying the Information Commissioner’s Office 6
9. Communication of a Personal Data Breach to the Subject 7
10. Post Breach Evaluation and Recording 8

Appendix 1 – Definitions 10

Appendix 2 – Data Breach Reporting Form 12

Appendix 3 – Flow Chart Showing Notification Requirements 13

#

# Introduction

* 1. East Ayrshire Leisure have a duty under data protection law and the General Data Protection Regulation (GDPR) to ensure that the personal data it processes is kept safe and secure. This procedure details how East Ayrshire Leisure will respond in the event of a personal data breach.
	2. No matter how careful we are in trying to ensure that all the personal data which East Ayrshire Leisure processes is kept securely and used with security in mind, the potential for a personal data breach will always remain. We need to have a system in place to enable us to deal with any such breach as quickly and as efficiently as possible.

#

# Purpose

* 1. This document puts into place a procedure for dealing with any breaches of personal data which may occur, focusing on the steps to be taken once a breach has been discovered, and the processes employees should follow.
	2. Instances of the loss of personal data are rare; however, the consequences to the reputation of the organisation and the potential impact on individual service users of the loss of personal information mean that we need to take swift and appropriate action in the event of a loss.
	3. In addition, the Information Commissioner’s Office (ICO) has the ability to impose significant fines on data controllers for serious contraventions of data protection law and the GDPR.
	4. The ICO also has the ability to serve an enforcement notice on a data controller if the ICO considers taking positive steps is also necessary to bring about compliance. It is possible to receive a fine and an enforcement notice.
	5. New timescales imposed under the GDPR legislation means that in certain circumstances a data breach must be reported (by our Data Protection Officer) within 72 hours of the beach becoming known to the organisation. If a breach is detected at 3pm on a Friday it needs to be reported by 3pm on the following Monday.
	6. This procedure aims to provide a consistent approach and follows guidance provided by the ICO. However, dealing with incidents of breaches of data is complex; there are many potential variables and a balanced judgement needs to be taken on a case by case basis.

# 3. Roles and Responsibilities

* 1. This procedure will be reviewed every three years, or earlier, if necessary.
	2. Senior Managers will be responsible for ensuring operational compliance with

 this procedure within their service areas and for seeking advice from the Data Controller,

 when appropriate.

* 1. East Ayrshire Leisure’s Data Controller is responsible for the provision of advice and guidance regarding this procedure and will liaise with East Ayrshire Council Data Protection Officer as required.

# 4. Ensuring Breaches Do Not Happen

4.1 The effects of personal data losses are not only felt by the individuals concerned, but also affect the efficiency of the service and the reputation of East Ayrshire Leisure as a whole.

* 1. It is important that all employees are aware of their responsibilities for handling

 personal information, keeping it secure and not disclosing it without proper

 cause. Senior Managers should ensure that all staff within their responsibility

 are familiar with the appropriate information governance and IT security policies

 and procedures.

* 1. East Ayrshire Leisure has a responsibility to ensure appropriate and proportionate security

 of the personal data it holds. This is covered by the 6th principle of the GDPR

 as detailed below:

*“*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’)”

* 1. To prevent East Ayrshire Leisure from being in breach of the requirements of Data

 Protection law and the GDPR all employees (whether permanent or temporary) and

 all third parties acting on behalf of East Ayrshire Leisure should be aware of their corporate

 and personal responsibilities to protect personal data from loss or theft.

* 1. Breaches may involve either criminal or civil liability, or both, depending on the

 circumstances, and may include both individual and corporate responsibility.

# 5. What is a Personal Data Breach?

* 1. Personal and Sensitive data is defined at Appendix 1. 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

 transmitted, stored or otherwise processed. This means that a breach is more

 than just losing personal data.

* 1. Such loss or release can occur in any of a number of ways:
* Loss or theft of equipment, which holds personal data e.g. laptops, tablets, CDs
* Loss or theft of hard copy documents
* Equipment failure
* Inappropriate access or unlawful access, allowing unauthorised use
* Human error
* Unforeseen incidents such as flood or fire
* Hacking attack
* Information obtained by surreptitious or deceptive means
* Information being released inappropriately

# 6. Types of Personal Data Breaches

6.1 Breaches can be categorised according to the following three information security principles.

* ‘Confidentiality breach’ - where there is an authorised or accidental disclosure of, or access to, personal data
* ‘Availability breach’ – where there is an accidental or unauthorised loss of access to, or destruction of, personal data
* ‘Integrity breach’ – where there is an unauthorised or accidental alteration of personal data

# 7. Dealing with a Breach

7.1 As soon as a breach has been identified, the employee concerned must report the incident immediately to their Line Manager, or a Senior Manager.

7.2 It is recommended that a Senior Manager is at that point nominated as ‘breach owner’ and that the Chief Executive is informed. **East Ayrshire Leisure’s Data Controller must be informed immediately and sent a completed Data Breach Incident Reporting Form (Appendix 2)**

7.3 It should be remembered that if a breach of personal data occurs where we are

 processing data on behalf of one of our partners, then the partner concerned

 must be notified immediately. Similarly, should a breach of personal data

 originate from a partner organisation, the effect of the breach on East Ayrshire Leisure

 should be assessed and the use of this procedure should be considered to

 protect the interests of East Ayrshire Leisure, customers and stakeholders.

7.4 If a breach is suspected to have taken place the following information will be

 required in order to assess the seriousness of the breach:

* The type of data involved
* How sensitive the data is
* If the data has been lost or stolen, whether there are any protections in place e.g. encryption
* What has happened to the data
* What could the data tell a third party about an individual
* The volume of data i.e. how many individuals’ personal data are affected by the breach
* Who are the individuals whose data has been breached
* What harm, if any, can come to those individuals
* Are there wider consequences to consider e.g. loss of public confidence, negative publicity, financial implications
	1. If after the initial assessment a breach has been clearly identified then an

 incident response team should be co-ordinated by the Data Controller.

This should include the key officers involved in the breach. It may also be worth alerting East Ayrshire Leisure’s Marketing & Development at this stage so they can be ready to deal with any media enquiries.

The key officers involved should be proportionate to the type of breach. For instance a minor breach may require the following:

* Line Manager
* Senior Manager (breach owner)
* Data Controller
* East Ayrshire Council IT Security Manager

A serious breach, whether in terms of size of breach, or sensitivity of information, should comprise the following:

* Chief Executive
* East Ayrshire Council Chief Governance Officer
* Senior Manager (breach owner)
* Data Controller
* East Ayrshire Council Data Protection Officer
* East Ayrshire Council IT Security Manager
* Marketing & Development Manager
	1. Responsibility rests with East Ayrshire Council Chief Governance Officer and the Chief Executive, in considering the action to be taken to:
* Protect the interests of the customer
* Ensure the continuing delivery of the service
* Protect the interests of East Ayrshire Leisure
* Meet the requirements of the GDPR in terms of informing the Information Commissioner’s Office (see section 8 below)
	1. Breaches will require not just an initial response to investigate and contain the

 situation but also a recovery plan including, where necessary, damage

 limitation. Establish who needs to be made aware of the breach and inform

 them of what they are expected to do to assist in the containment exercise.

 This could be isolating or closing a compromised section of the network, finding

 a lost piece of equipment, or simply changing access codes. Establish whether

 losses can be recovered and damage can be limited.

* 1. Fully assess the risk in terms of the potential adverse consequences for individuals. How serious or substantial are the consequences and how likely are they to happen?

# 8. Notifying the Information Commissioner’s Office (ICO)

8.1 The GDPR places a duty on all organisations to report certain types of data

 Breach to the Information Commissioner’s Office.

8.2 In the case of a personal data breach East Ayrshire Leisure shall without undue delay and,

 where feasible, not later than 72 hours after having become aware of it, notify

 the ICO, **unless the personal data breach is unlikely to result in a risk to the**

 **rights and freedoms of natural persons.** Where the notification to the ICO is not

 made within hours, it shall be accompanied by reasons for the delay.

 8.3 The GDPR states that a personal data breach should be reported to the ICO if

 the breach is likely to result in a risk to the rights and freedoms of the

 individuals concerned. By this it means discrimination, damage to reputation,

 financial loss, loss of confidentiality or any other significant economic or social

 disadvantage. It also requires that this is done on a case by case basis**. If**

 **there is not a risk to rights and freedoms, the ICO does not need to be notified.**

 8.4 After carrying out a full assessment of the risk, the decision as to whether or not

 to inform the ICO would rest with the East Ayrshire Council Chief Governance Officer and Chief Executive.

* 1. If the decision is to notify the ICO, East Ayrshire Council Data Protection Officer will act as liaison with the ICO.
	2. The Senior Manager in conjunction with the Head of Corporate Services will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures or require any remedial training or support.
	3. The notification referred to in paragraph 8.2 shall at least:
1. Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
2. Communicate the name and contact details of the East Ayrshire Council Data Protection Officer or other contact point where more information can be obtained
3. Describe the likely consequences of the personal data breach
4. Describe the measures taken or proposed to be taken by East Ayrshire Leisure to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
	1. Where, and in so far as, it is not possible to provide the information to the ICO at the same time, the information may be provided in phases without undue further delay.
	2. East Ayrshire Leisure shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the ICO to verify compliance with the GDPR.
	3. Failing to notify a breach when required to do so can result in a significant fine; this is at the discretion of the ICO.

# 9. Communication of A Personal Data Breach to the Data Subject

9.1 The incident response team will determine whether to communicate the data breach to the data subject. This will depend on the circumstances of the case and whether the data breach is likely to result in a high risk to individuals. The incident response team will also determine the method by which to communicate the breach to affected individuals, with particular care being placed on the communication when the breach affects the personal safety of a child or vulnerable adult.

9.2 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, East Ayrshire Leisure shall communicate the breach to the data subject without delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are:

* Discrimination
* Identity theft or fraud
* Financial loss
* Damage to reputation

9.3 When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

9.4 Further information regarding the methodology of assessing the risk to the data subject can be found in the Article 29 Guidelines on Personal data breach notification under Regulation 2016/679 Section IV at the link below.

 [Article 29 Breach Reporting](http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiE27_2i6XZAhUMBcAKHarxD3gQFgguMAA&url=http%3A%2F%2Fec.europa.eu%2Fnewsroom%2Fdocument.cfm%3Fdoc_id%3D47741&usg=AOvVaw0Zb02JvMR84bVF9Jz_ssOo)

9.5 The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of paragraph 8.7.

9.6 The communication to the data subject shall not be required if any of the following conditions are met:

1. East Ayrshire Leisure has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
2. East Ayrshire Leisure has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise
3. It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

9.7 East Ayrshire Council Data Protection Officer will consider consulting the ICO to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

9.8 Consideration also needs to be given to any prospective equality issues that may arise from a breach e.g. the vulnerability of an individual affected by the breach.

#  Post Breach Evaluation and Recording

10.1 Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on ‘business as usual’ may not be acceptable if systems, policies or allocation of responsibilities were found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and recorded so East Ayrshire Leisure can be seen to have reacted in a responsible manner.

10.2 Those investigations into the cause of the loss of data should consider any staff

 capability or training issues that may be indicated and where appropriate, action

 may be considered under East Ayrshire Leisure’s disciplinary procedure.

 10.3 If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future.

10.4 East Ayrshire Council Data Protection Officer and East Ayrshire Leisure Data Controller will record all breaches (and actions taken) in a data breach register.

* 1. The Data Protection Officer will track compliance with agreed actions and provide an update to the Corporate Information Governance Group so that any learning points can be distributed across East Ayrshire Leisure.

**Record of Change**

|  |  |
| --- | --- |
| **Date Reviewed** | **Date of next review** |
| Aug 2019 | Aug 2020 |

# Appendix 1- Definitions

**Personal data**

‘Personal data’ means any information relating to an identified or identifiable living individual (‘data subject’)

‘Identifiable living individual’ means a living individual who can identified, directly or indirectly, in particular by reference to:

1. an identifier such as a name, an identification number, location data or an online identifier, or
2. one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

**Special category (sensitive) personal data**

‘Special category (sensitive) personal data’ means data about:

* Racial or ethnic origin
* Political opinions
* Religious/philosophical beliefs
* Trade union
* Processing of biometric/genetic data to identify someone
* Health
* Sex life or sexual orientation

**Data subject**

‘Data subject’ means the identified or identifiable living individual to whom personal data relates.



21/11/18

**Appendix 2 - Data Breach Incident Reporting Form**

|  |  |
| --- | --- |
| Reporting Employee Name: | Tel : |
| Line Manager Name : | Tel : |

|  |
| --- |
| How was the breach discovered (include date of the breach)? |

|  |
| --- |
| How would you categorise the breach (please tick where applicable)? |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Loss |  | Theft |  | Unauthorised disclosure |  |
| Unauthorised access |  | Unauthorised use |  | Human error |  |

|  |
| --- |
| What information was involved and who did it relate to (how sensitive is the data)? What happened to the data? |

|  |
| --- |
| How was the information held (e.g. online, on a laptop, contained within a letter or email)? Was the information protected e.g. encrypted? |

|  |
| --- |
| Explain the consequences of the breach (include info about who has had access to it and/or what the potential effect of the breach may have on the person the information is about) |
| Provide a description of the immediate measures taken to mitigate the impact of the breach |
| Explain what proposed measures/actions you intend to put in place to prevent the breach occurring in the future |

|  |  |
| --- | --- |
| When was the breach reported to line management? |  |
| When was the breach reported to the Senior Manager? |  |
| When was the breached reported to the Data Controller |  |
| When was the breach notified to East Ayrshire Council Data Protection Officer |  |

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Forward the completed proforma to East Ayrshire Leisure’s Data Controller at EALInformationgovernance@eastayrshireleisure.com

**Appendix 3 - Flow chart showing notification requirements**

Data Breach Incident Response Team notified of a personal data breach and assesses risk to individuals.

Service detects/is made aware of a security incident and establishes if personal data breach has occurred.

he require

Yes

No

No requirement to notify individuals.

Is the breach likely to result in a high risk to individuals’ rights and freedoms?

Yes

All breaches recordable under Article 33(5) of the GDPR. Breach should be documented and record maintained by East Ayrshire Leisure.

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.

Is the breach likely to result in a risk to individuals’ rights and freedoms?

Notify the ICO

No requirement to notify ICO or individuals

No