Personal Data Breach Policy

Annex 1 – Data Breach Checklist

Step	Action	Notes
A	**Containment and recovery**	**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Data Protection Manager and Managing Director to ascertain the severity of the breach and determine if any personal data is involved.	*To oversee full investigation and produce report. If personal data has been breached contact the ICO as appropriate.*
2	Identify the cause of the breach and whether it has been contained. Ensure that the possibility of any further data loss is removed or mitigated as far as possible.	*Establish what steps can or need to be taken to contain the breach from further data loss. This may involve actions such as taking systems offline or restricting access to systems to a limited number of staff until more is known about the incident.*
3	Determine whether anything can be done to recover any losses and limit any damage that may be caused.	*Such as physical recovery of data/equipment or where corrupted, through use of back-ups.*
4	Where appropriate, the Managing Director to inform the police.	*Such as in the case of stolen property, fraudulent activity, offence under the Computer Misuse Act.*
5	Ensure all key actions and decisions are logged and recorded.	
B	**Assessment of Risk**	***To identify and assess the on-going risks that may be associated with the breach***
6	What classification of data is involved?	• *Public – any information published or available publicly (in the public domain)* • *Internal – any information circulated within Family Wise Ltd only, including information which is only accessible to certain employees* • *Confidential – any personal or confidential information Protected – highly sensitive information.*
7	What volume of data is involved?	
8	How sensitive is the data?	*Special category personal data?*
9	What has happened to the data?	*e.g., if the data has been stolen, it could be used for purposes which are harmful to the individuals to whom it relates.* *If damaged this poses a different type and level of risk.*

10	If the data was lost/stolen, were there any measures in place to prevent access/misuse?	*Encryption of the data or device?*
11	If the data was damaged/corrupted/lost, were there measures in place to mitigate the impact of the loss?	*Back-up strategy?*
12	How many individuals' personal data affected?	
13	Who are the individuals whose data has been compromised?	*Staff, applicants, clients, customers, service users or suppliers*
14	What could the data tell a third party about the individual? Could it be misused?	*Consider this regardless of what has happened to the data.*
15	Is there actual/potential harm that could come to any individuals?	*Are there risks to:* • *Physical safety* • *Emotional wellbeing* • *Reputation* • *Finances* • *Identity* • *Or a combination of these and other private aspects of their life?*
16	Are there wider consequences to consider?	*Are there risks to reputation of the company?*
17	Are there others who might advise on risks/courses of action?	*For example - If bank account details have been lost, consider contacting the banks themselves for advice on anything they can do to help prevent fraudulent use.*
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions**
18	Are there any legal, contractual or regulatory requirements to notify?	*For example any contractual obligations?*
19	Can notification help the company meet its security obligations under the GDPR?	*Prevent any unauthorised access, use or damage to the data or loss of it?*
20	Can notification help the individual?	*Could individuals act on the information provided to mitigate risks (e.g. by changing their password or monitoring their account)?*
21	If a large number of people are affected or there are very serious consequences, inform the ICO.	
22	Consider the dangers of 'over notifying'.	*Not all incidents will warrant notification – take a pragmatic approach to notification.*
23	Consider who needs to be notified, what you will tell them and how this will be communicated.	*Always consider the security of the medium of communication as well as the urgency.*

		Annex 3 is to assist in reporting a breach to the ICO.
24	Consult the ICO guidance on when and how to notify it about breaches.	*Guidance available from:* Report a breach | ICO *Further information to help assess the risk is provided in Annex 2.*
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	*e.g. police, insurers, professional bodies, trade unions, website/system providers, bank/credit card companies.*
D	**Evaluation and Response**	**To evaluate the effectiveness of the company's response to the breach**
26	Establish where any present or future risks lie.	
27	Consider the data and contexts involved.	*What data is held, its extent, sensitivity, where and how it is stored, how long it is kept.*
28	Consider and identify any weak points in existing security measures and procedures.	*In relation to methods of storage and/or transmission, use of storage devices, levels of access, system/network protection.*
29	Consider and identify any weak points in levels of security awareness/training.	*Fill in any gaps through training or specific advice.*
30	Report on findings and implement recommendations.	*Report to Managing Director.*