Annington Personal Data Breach Policy

1. Introduction

1.1 **Annington's Data Protection Lead is Sarah Jury (email: dataprotection@annington.co.uk; tel: 07468 495 662). The Data Protection Lead should be your first point of contact to report any Personal Data breach or if you have any other queries or concerns about this policy or about dealing with Personal Data.**

1.2 Annington Limited, and all Annington group companies ("**Annington**", "**we**", "**us**" or "**our**") have obligations under Data Protection Legislation regarding how we protect the personal data we hold.

1.3 Annington collects, holds, processes, and shares personal data – sensitive information that needs to be suitably protected.

1.4 Annington seeks to ensure that personal data is protected from "data breaches".

1.5 However, if a data breach occurs, Annington has an obligation to report it to regulators and/or individuals in certain circumstances. Where required to do so, Annington must notify the regulator of a data breach 'without undue delay' and at the latest within **72 hours** of **anyone** in the business becoming aware of the data breach incident. Where a data breach is required to be reported to individuals, this must be done **as soon as possible** following awareness by the business.

1.6 Compromise of personal data confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial costs. Failure to notify a data breach to the regulator and/or individuals, where required, can result in severe financial penalties (for the organisation, this could be up to £17.5 million or 4% of the total annual worldwide turnover, whichever is higher), along with reputational damage and claims from affected individuals for unlimited compensation.

1.7 Annington relies on the vigilance and prudence of its employees, partners, contractors and employees to comply with its legal obligations. If you discover anything that you think could be an actual or 'near miss' data breach relating to personal data, you **must** notify the Data Protection Lead **immediately**.

2. Purpose and Scope

2.1 Annington is obliged under Data Protection Legislation (which includes the Data Protection Act 2018 (the "**DPA**") and the UK General Data Protection Regulation (the "**UK GDPR**")) to have a framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

2.2 This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breaches.

2.3 This policy relates to all personal data held by Annington, regardless of its format (physical or digital).

2.4 This policy applies to all staff at Annington. This includes all Annington employees and temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Annington.

2.5 The objective of this policy is to:

- 2.5.1 contain any data breaches;
- 2.5.2 minimise the risk associated with any data breach and consider what action is necessary to secure personal data; and
- 2.5.3 prevent further data breaches.

3. Definitions

3.1 A "**data breach**" in the context of this policy is an event or action which has compromised the confidentiality, integrity or availability of personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. For the purposes of this policy, data breaches include both confirmed and suspected incidents.

3.2 Examples of data breaches may include, but are not restricted to, the following (where personal data is

involved):

3.2.1 loss or theft of equipment on which such data is stored (e.g. loss of laptop, USB stick, smart phone iPad / tablet device, or paper record);

3.2.2 malicious incidents such as a cyber-attack, phishing attack, ransomware attack and information obtained by deception;

3.2.3 loss of availability of personal data, such as through its corruption, being wiped or being extracted from a system;

3.2.4 system failure;

3.2.5 unauthorised use of, access to or modification of data or information systems;

3.2.6 attempts (failed or successful) to gain unauthorised access to information or IT system(s);

3.2.7 unauthorised disclosure of any personal data or sensitive / confidential data;

3.2.8 website defacement;

3.2.9 hacking attack;

3.2.10 unforeseen circumstances such as a fire or flood (which for example may impact hard copies of personal data, or servers holding personal data); or

3.2.11 human error, such as giving personal data to the wrong person via email.

3.3 "**Personal data**" is information (in any format) that relates to a living individual who can be identified from that information, either on its own or when it's combined with other information held by us.

3.4 "**Data subject**" means the individual to whom the personal data relates. For simplicity, in this policy, we sometimes refer to these people as 'individuals'.

3.5 "**Special personal data**" (sometimes referred to as 'sensitive personal data' or 'special category data') is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal convictions and offences, genetic data, biometric data (where it's processed to uniquely identify someone), data concerning health or data concerning someone's sex life or sexual orientation.

4. Reporting a data breach

4.1 Every member of the Annington team and its suppliers and contractors has a critical role to play in making sure that we manage the data entrusted to us safely, sensitively and in compliance with the law. Everyone is responsible for reporting data breaches and information security incidents immediately to the Data Protection Lead and IT Services using the email address dataprotection@annington.co.uk and on 07468 495 662.

4.2 If the data breach occurs or is discovered outside normal working hours, it must still be reported immediately after you have become aware of it. The deadlines under Data Protection Legislation run 24 hours a day, 365 days a year, so time is of the essence.

4.3 You should report any concerns about a data breach or potential data breach even if it was an accidental issue or due to an error, or if the incident may have occurred because of someone else (e.g. another member of staff, or a supplier), as reporting it straightaway can mean that damage can either be prevented or limited. The report must include full and accurate details of the data breach, when the data breach occurred (dates and times), who is reporting it, the nature of the breach and affected data, and how many individuals are involved. An Incident Report Form should be completed as soon as possible as part of the reporting process (refer to Appendix 2). Even if you do not have all the details, report the data breach as soon as you can, as the other details can follow as soon as they become available.

4.4 Data breaches should be kept confidential and details should not be shared with anyone but your line manager, the Data Protection Lead, and the IT Services team until you are informed otherwise.

4.5 Any breach of Data Protection Legislation and/or this policy, including where incidents are knowingly not reported or are 'covered up', may result in disciplinary action.

5. Containment and recovery

5.1 In the event that a potential breach or incident is reported, the Data Protection Lead and the Head of

IT will:

5.1.1 firstly determine if the data breach is still occurring. If so, the appropriate steps will be taken immediately to contain or stop the effect of the data breach.

5.1.2 Make an initial assessment to establish the severity of the data breach and the likelihood and severity of the resulting risk to people's rights and freedoms.

5.1.3 stablish whether:here is anything that can be done to recover any losses and limit the damage the data breach could cause.

5.1.4 establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

5.1.5 Seek advice from experts outside Annington where needed. Care will be taken to protect the confidentiality of any information before bringing in external IT/forensics teams.

5.1.6 determine the course of action to be taken to ensure a resolution to the incident.

6. Investigation and risk assessment

6.1 An investigation will be undertaken by the Data Protection Lead immediately and wherever possible, within 24 hours of the data breach being discovered / reported.

6.2 The Data Protection Lead will likely need the help from anyone who reported or provided information about the data breach at this stage.

6.3 The investigation will need to take the following into account:

6.3.1 the type of data involved;

6.3.2 its sensitivity;

6.3.3 the protections in place (e.g. encryptions);

6.3.4 what has happened to the data (e.g. has it been lost or stolen);

6.3.5 whether the data could be put to any illegal or inappropriate use;

6.3.6 data subject(s) affected by the data breach, number of individuals involved and the potential effects on those data subject(s);

6.3.7 whether there are wider consequences to the data breach.

7. Notification

7.1 The Data Protection Lead, in consultation with relevant colleagues, will establish whether the Information Commissioner's Office needs to be notified of the data breach (based on whether the data breach is likely to result in a risk to the rights and freedoms of individuals), and if so, notify them without undue delay and within 72 hours of becoming aware of the data breach. Details of what notifications will include, the elements to consider when deciding whether to notify individuals and what notification to individuals will include can be found in Appendix 1:

7.2 If it is determined that personal data has been affected, requiring notification to affected individuals: Specific and clear advice will be given on what they can do to protect themselves, and details of action already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact Annington for further information or to ask questions on what has occurred.

7.3 The Data Protection Lead must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

7.4 The Data Protection Lead will consider whether the PR team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

7.5 A record will be kept of any data breach, regardless of whether any notification was required.

8. Evaluation and response

8.1 Once the initial incident is contained, the Data Protection Lead will carry out a full review of the causes of the data breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

8.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

8.3 The review will consider:

8.3.1 where and how personal data is held and where and how it is stored;

8.3.2 where the biggest risks lie including identifying potential weak points within existing security measures;

8.3.3 whether methods of transmission are secure; sharing minimum amount of data necessary;

8.3.4 staff awareness; and

8.3.5 implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

8.4 If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Annington Board.

9. Policy Review

9.1 This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

9.2 This is version 1.2 of the policy, October 2023.

10. Appendix 1

10.1 Notification of a data breach will include:

10.1.1 details of the data subject(s) affected by the data breach, the number of individuals involved and the potential effects on those data subject(s);

10.1.2 whether there are wider consequences to the data breach;

10.1.3 the nature of the 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;

10.1.4 the name and contact details of the Data Protection Lead so more information can be obtained;

10.1.5 the likely consequences of the data breach;

10.1.6 the measures taken or proposed to be taken by Annington to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10.2 Every incident will be assessed on a case by case basis; however, the following will need to be considered by the Data Protection Lead when deciding whether to notify individuals whose personal data is involved in the data breach:

10.2.1 whether the data breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection Legislation (see: Personal data breaches | ICO);

10.2.2 whether notification of affected individuals would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);

10.2.3 whether notification of affected individuals would help prevent the unauthorised or unlawful use of personal data;

10.2.4 whether there are any legal / contractual notification requirements; and

10.2.5 the dangers of over notifying (as not every incident warrants notification and over notification may cause disproportionate enquiries and work and unnecessary concern).

10.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description in clear and plain language of:

10.3.1 how and when the data breach occurred;

10.3.2 the nature of the data breach;

10.3.3 the data involved;

10.3.4 the name and contact details of the Data Protection Lead so more information can be obtained;

10.3.5 the likely consequences of the data breach; and

10.3.6 the measures taken or proposed to be taken by Annington to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

11. **APPENDIX 2**

PERSONAL DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please email the Data Protection Lead and the helpdesk immediately and then complete Section 1 of this form and email it to the helpdesk.

Section 1: Notification of Data Security Breach	**For use by the person who identified the data breach**
Date and time incident was discovered:	
Date(s) and time of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information affected, including: • how the incident occurred • how you discovered the data breach • whether the data breach is ongoing • whether the data breach was caused by a cyber attack • whether any systems/equipment has been affected • whether you believe the information has been lost or stolen • how serious you think the data breach is • why you think the breach has occurred	
Details of the categories of data subjects that have been or are likely to have been affected by the data breach (e.g. staff, suppliers, property owners, individuals who rent properties etc.)	
Number of Data Subjects affected or likely to be affected, if known:	
What personal data has been placed at risk, how vulnerable are affected individuals, how easily could the details be exploited (for example, to identity theft, fraud, or any equivalent), whether individuals are likely to be harmed or hurt due to the disclosure/data breach, and how easy is it to identify individuals from the affected personal data?	

Brief description of action taken at the time of discovery (if any):	
If the data breach involved a cyber incident, do you consider that Annington has recovered from the data breach (with all personal data in the same state it was before the data breach)? If not, do you think is it possible to restore all personal data to the same state?	
For use by the Data Protection Lead	
Received by:	
On (date and time):	
Forwarded for action to:	
On (date):	

Section 2: **Assessment of Severity**	
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost? Has it been damaged or corrupted? If so, were there protections in place to lessen the impact.	
How much data has been lost? If the data was on a laptop or other device which has been lost/stolen: how recently was the device backed up onto central IT systems? Is it a work device or personal device? Is it encrypted? What other protections are in place to prevent access or misuse, if any?	
Is the information unique (Annington's only copy of it – or is there a back-up copy)? Will its loss have adverse operational, research, financial, legal, liability or reputational consequences for Annington or affected individuals or third parties?	
How many data subjects are affected or are likely to have been affected? If the data breach was a cyber-attack and the number of affected data subjects is not known, please provide an estimate of the maximum possible number that could be affected or the total customer base.	
Please describe any potential impact you envisage the data breach may have, or has already had, on individuals, e.g. do you consider there is a risk of potential misuse by a third party and that harm could come to any individuals because of it? How easy is it to identify data subjects from the data?	
Is the data bound by any contractual security and/or confidentiality arrangements?	
What is the nature of the sensitivity of the data?	
• Details of the categories of **HIGH RISK** personal data that has been, or may be, affected (**please note all that apply**):**Special categories personal data** (as defined in the Data Protection Legislation) relating to a living, identifiable individual's: a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) trade union membership; d) genetic data; e) biometrics (where used for ID purposes); f) health; g) sex life or sexual orientation; h) criminal allegations, convictions, offences;	

• Basic personal identifiers, e.g. name, contact details or identification data, e.g. usernames, passwords; • Official documents, e.g. driving licences; • Location data, e.g. coordinates; • Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas; card details; • Personal information relating to vulnerable adults and children; • Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed; • Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals. • Security information that would compromise the safety of individuals if disclosed (for example, MoD staff details).	

Section 3: **Action taken**	
Incident number	
Report received by:	
On (date):	
Action taken by responsible officer/s:	
Has incident been recorded in the data breach risk register?	**Yes/No** **If YES, recorded on (date):**
Was incident reported to Police?	**Yes/No** **If YES, notified on (date):**
Was incident reported to insurers?	**Yes/No** **If YES, notified on (date):**
Follow up action required/recommended:	
Reported to other internal stakeholders (details, dates):	
For use of Data Protection Lead and/or Lead Officer:	
Notification to ICO	**YES/NO** **If YES, notified on: Details:** **If NO, summary reasons why not:**
Notification to data subjects (only relevant where ICO notified but not otherwise)	**YES/NO** **If YES, notified on: Details:** **If NO, summary reasons why not:**
Notification to other external, regulator/stakeholder	**YES/NO** **If YES, notified on: Details:**