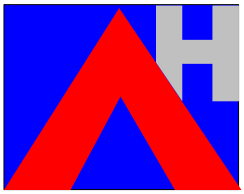
ANNINGTON

Data Protection Policy and Procedure

Last updated: October 2023

Minor changes made 13/09/23



Author(s)	Tim Bond, Sarah Jury, Holly Miller
Address	1 James Street London W1U 1DR

Table of Contents

1 Introduction

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 if you have any queries or concerns about this policy or about dealing with Personal Data.

Data protection and related ePrivacy laws regulate the use of "Personal Data" and give rights to individuals, including employees about whom "Personal Data" is obtained or processed, whether manually or electronically. These laws give people rights regarding how their Personal Data is processed. These rights apply to you, as well as to every individual whose Personal Data you process while working for us. This policy does not distinguish between hard copy and electronic data.

Annington Limited, and all Annington group companies ("**Annington**", "**we**", "**us**" or "**our**") have obligations under these data protection laws regarding how we treat the Personal Data we hold, what we do with it and who we share it with. This policy describes the requirements for the processing of Personal Data by Annington to meet its legal obligations and what your responsibilities are to ensure that we comply with them. It applies to all Annington group companies and all employees, consultants, contractors, agency workers and temporary staff using Annington Personal Data as a result of their work for Annington. Everyone who works for us, whether as our employee or in another capacity as part of our business operations, must comply with this policy when processing Personal Data. In this policy references to "**you**" mean anyone that processes Personal Data for us, regardless of their employment status. This policy applies whenever you handle Personal Data about anyone else, including colleagues, job applicants, customers and suppliers who are individuals or partnerships and individual contacts at company customers and company suppliers.

Annington is committed to fulfilling its obligations under data protection and privacy legislation in respect of all processing of Personal Data in connection with its business and in so doing meeting the expectations of our employees, customers and suppliers.

The key data protection laws which apply to Annington are the Data Protection Act 2018 ("**DPA**"), the UK General Data Protection Regulation ("**UK GDPR**"), together with the Privacy in Electronic Communications (EC Directive) Regulations 2003 ("**PECR**").

Annington depends on you to help it comply with its obligations under these laws. It will be important to ensure that you are aware of and comply with all relevant Annington policies and procedures and attend any training provided.

Data protection legislation is enforced in the UK by the Information Commissioner's Office, who can investigate complaints, audit our use of Personal Data and take action against us (and in some cases against you personally) for breach of this legislation. Breaches of the law can result in serious consequences for Annington and you personally, including preventing business as usual operations (by preventing us from using Personal Data), substantial fines, compensation claims, damage to reputation, loss of business and criminal prosecution. The impact on individuals of any breach must not be forgotten or underestimated, as it may involve intrusion, distress, identity theft, fraud and financial loss.

Everyone at Annington has a responsibility to read and comply with this policy and any other policies referred to in it, as well as to attend mandatory data protection training that may be provided. It is important that you understand how important Data Protection is and what is expected of you - please read this policy carefully and contact your line manager if you have any queries or concerns.

2 Definitions

2.1 What is 'Personal Data'?

Personal Data is information (in any recorded format) which relates to a living individual who can be identified from that information, whether on its own or when combined with other information held by us. Common examples of Personal Data which may be used by Annington in its day to day business include names, addresses, telephone numbers and other contact details, bank details, credit history, CVs, performance reviews, salaries and statements of opinion or intention regarding individual employees, tenants, occupiers, management agents or other individuals. It also includes marketing preferences, email addresses and records of behaviour of individuals.

When considering whether data allows a person to be identified, you must consider it as a jigsaw piece and whether, with all the other jigsaw pieces Annington holds (or is held on behalf of Annington) in respect of that person, when two or more are put together they would enable identification of the person. The definition of Personal Data is broad, and increasingly – as technology enables us to identify individuals more easily – more data is likely to be regarded as Personal Data.

Some specific types of Personal Data are classed as sensitive or special Personal Data ("**Special Personal Data**") under the data protection legislation. This includes Personal Data revealing or concerning -

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health;
- a natural person's sex life or sexual orientation;
- criminal convictions and offences;
- biometric data for the purpose of uniquely identifying a natural person; or
- genetic data.

There are special obligations under the data protection legislation with which Annington must comply when processing Special Personal Data to limit its collection and use and to ensure it is treated more securely than other details.

Annington also needs you to take special care of other Personal Data which could either expose them to criminal behaviour (e.g. bank details, credit card information, identity documentation) or the disclosure of which could put them or those associated with them at risk or cause them distress (e.g. information about children or private personal circumstances).

2.2 What is 'Processing'?

Annington will be "processing" Personal Data if it collects Personal Data and/or carries out any operation relating to that information such as retaining that data after collection, altering or deleting it, storing, using, destroying, accessing, downloading, reviewing or disclosing it to another party and/or transferring it to another jurisdiction.

It is irrelevant whether the information is stored as a hard copy record within a filing system or is electronically processed.

Sending Personal Data from one company to another, or allowing it to be shared with them or seen by them is a disclosure. There are no different rules to make it easier to share Personal Data between Annington group companies and you must comply with Annington guidance before doing so.

Annington has put in place an intra-group data sharing agreement to comply with its obligations.

3 The Rules for Processing Personal Data

There are six main data protection principles, which we must follow in respect of all Personal Data we process. It is essential that you also comply with them when processing Personal Data for us.

The principles are that Personal Data must be:

- processed lawfully, fairly and in a transparent manner (see paragraph 3.2).
- processed only for the specified, explicit and legitimate purpose(s) we collect it for (see paragraph 3.3).
- adequate, relevant and limited to what we need in relation to the purpose(s) we collect it for (see paragraph 3.4-3.5).
- kept accurate and kept up to date (see paragraph 3.6).
- kept for no longer than necessary in relation to the purpose(s) we process it (see paragraph 3.7).
- kept secure (see paragraph 3.9).

We may be asked to demonstrate that we have complied with the data protection principles at any time. Therefore, part of your role is therefore to ensure that you help the Data Protection Lead by letting them know what Personal Data you process and how the processing complies with those principles. The Data Protection Lead keeps these details in the Data Retention Guidelines.

Disclosure and use of Personal Data held by Annington is governed by these rules in order to ensure compliance with data protection legislation and in the interests of privacy, employee and customer confidence and good employee and customer relations. Annington adopts a privacy by design and default approach to its collection and use of Personal Data. Everyone is expected to contribute to this.

3.1 Notification and Prior Approval

Annington is required to notify the Information Commissioner about the processing of Personal Data carried out by Annington, which it has done and has appointed a Data Protection Lead to review and co-ordinate the processing of Personal Data within Annington in accordance with the UK GDPR and recommended good practice. Annington is only permitted to process Personal Data within the scope of its notification.

If you want to collect additional Personal Data, use Personal data for any new reason, appoint a new service provider, or procure a new IT system or technology, please advise the Data Protection Lead in advance so this can be covered in the notification (if agreed appropriate) and assessed to ensure lawfulness. Do not start undertake any of these actions or activities without their prior written approval.

3.2 Use of Personal Data must be Fair, Lawful and Transparent

Fairness and transparency

Annington must ensure that:

- wherever possible, individuals reasonably expect the use which Annington will make of their Personal Data; and

- individuals are advised of the Personal Data which will be obtained and the purposes for which the Personal Data may be used, in most cases prior to any collection of such Personal Data ("**Fair Notice**").

As part of Fair Notice we must give individuals very specific information about how we process their Personal Data, to ensure that our processing is fair and transparent. This information is often referred to as a fair processing notice (FPN) or privacy notice. For example, the Fair Notice should identify the responsible Annington company dealing with their Personal Data and should also explain to whom the Personal Data may be disclosed e.g. other group companies or the taxation authorities, from whom other data may be obtained e.g. referees for job applicants; and where the Personal Data may be sent to outside the UK. You must ensure that you only use the appropriate Annington approved Fair Notices.

You should contact the Data Protection Lead to discuss your Fair Notice requirements before collecting any Personal Data in connection with any projects, products or services you are designing, offering or providing. We should provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. In most circumstances, we should provide the information at the time the individual's Personal Data is collected. If the information is not received directly from the individual concerned, then Annington must ensure that the individual is given all the relevant information above as soon as possible (at the latest within a month and before any disclosure or transfer of their details, or contact with the individual) and that Annington has authority to use this information.

We have set out below the procedures you should follow in respect of each channel by which we collect Personal Data:

- Our websites and other digital platforms. You should make sure that the relevant website or digital platform contains a permanently visible link to our online Privacy Policy.

- Paper – subjects should receive the appropriate Fair Processing Notice.

You must not buy in or sell any Personal Data about individuals (including marketing lists), or carry out any activities involving any data enhancement or enrichment or matching, without prior written approval from the Data Protection Lead.

Lawful

We must always have a "lawful basis" for processing Personal Data. The lawful bases which are most likely to be relevant to our processing are where:

- the processing of the individual's Personal Data is **necessary to perform a contract** with that individual or to take steps at the request of the individual before entering into a contract.
- the processing **is necessary to comply with a legal obligation** to which we are subject.
- the processing is **necessary in order to protect the vital interests** of an individual.
- the processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in us.
- the processing is **necessary for our legitimate interests**, provided those interests are not overridden by the individual's interests, rights or freedoms.

Individuals have a right to object to our processing of their Personal Data where we are relying on this lawful basis for that processing (see paragraph 3.8):

- the individual has given his or her **consent** to the processing - consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes in order to be valid. This means that the use of pre-ticked tick boxes (or other methods which assume that silence constitutes consent) will not be sufficient. Where the individual is asked to give a written declaration of consent, the request should be clearly distinguishable from other matters and in an intelligible and easily accessible form, using clear and plain language. Individuals can withdraw their consent at any time (see paragraph 3.8) and we have to make sure it's easy for them to do so.

We must make sure that we let people know which lawful basis we are relying on for any processing of their Personal Data (see the beginning of this paragraph).

Special Personal Data

An extra layer of rules apply when we process Special Personal Data (as defined in paragraph 2.1 above).

We still need to have a lawful basis (as referred to above) for processing Special Personal Data, but we also need an additional justification for processing it. The justifications that are most likely to be relevant are:

- where the individual has given their explicit consent to the processing, or

- where the processing is necessary for employment or social security purposes (N.B. This policy is also our policy for the purpose of Part 4 of Schedule 1 of the Data Protection Act 2018).

Please see paragraph 3.4 below for further conditions on processing Special Personal Data.

If you have any questions or concerns in relation to processing Special Personal Data, you should contact the Data Protection Lead.

3.3 Personal Data must Only be Used for Specified and Explicit Lawful Purposes (Purpose Limitation)

Annington must only use Personal Data for a lawful purpose (see paragraph 3.2 above) and in the ways described in the Fair Notice given to the individual concerned (and any relevant Annington notification to the Information Commissioner), unless otherwise permitted by the data protection legislation, and it mustn't be further processed for reasons which aren't compatible with those purposes.

If you have any doubt as to whether your proposed use of Personal Data is justified, you must check in advance with the Data Protection Lead.

New processing purposes must be approved in writing by the Data Protection Lead before that processing takes place and may need Annington to update individuals on such new proposed use before it can commence. This includes anonymisation of Personal Data and use for research or analysis.

Provided that the identification of individuals cannot be ascertained or is not disclosed, truly anonymous aggregated or statistical information may be used outside the data protection legislation e.g. to respond to any legitimate internal or external requests for data such as surveys or manpower figures. However, please liaise with the Data Protection Lead if you wish to do so beforehand to make sure your proposed use is lawful.

3.4 Use of Personal Data must be Justified

Annington can only use Personal Data (as defined in paragraph 2.1 above) within specific limited conditions set out in the data protection legislation (as set out in paragraph 3.2 above). It is important that use of Personal Data by Annington is permitted by data protection legislation and in most cases that means that use must be "necessary" for a specific purpose, on a proportionate and need to know and do basis.

Normally this will be on the basis that the use is necessary to perform a contract with the individual concerned, to comply with a relevant law, or where it is necessary for a legitimate business use and is proportionate so that there is no unwarranted prejudice to the individual concerned.

In addition, extra care is needed when you process Special Personal Data and extra controls apply to any use of Special Personal Data because its misuse would cause more damage and distress if it is received by an unintended recipient or if it goes astray. Therefore, you should not email it or disclose it unless you take steps to encrypt or otherwise secure it. In relation to staff, Annington may use Special Personal Data to comply with its mandatory employment related legal obligations e.g. for health and safety or to pay sickness pay. Otherwise, Annington must limit its collection and use of such details and may need to obtain the voluntary, informed, explicit written consent from an individual (in the appropriate approved Annington format) to process Special Personal Data. If use of such details is not mandatory by law, obtain approval from the Data Protection Lead before collecting and using such details. Once a valid form of explicit consent has been obtained, you must comply with it. Annington must not process Special Personal Data otherwise (unless in an emergency situation to save life or prevent serious harm).

Special Personal Data must not be sent by fax unless it is to a confidential or direct individual (rather than general or public) fax number, the fax is marked confidential and the recipient has been notified in advance of it being sent and safe receipt is confirmed. If Special Personal Data has to be sent by email, you must liaise with the Data Protection Lead to ensure appropriate security (including encryption, where appropriate) can be afforded to the information before it is sent.

Annington will only rely on individual consent to Personal Data use in limited cases approved in advance by the Data Protection Lead and based on appropriate Annington approved forms of consent.

You must ensure that your use of Personal Data complies with the relevant Fair Notice and/or consent obtained and you must not request individual consent to use Personal data in other cases, or use other forms of consent.

3.5 The Use of Personal Data must be Adequate, Relevant and Necessary (Data Minimisation)

Personal Data processed by Annington must be adequate, relevant, not excessive for Annington's legitimate business purposes and necessary in relation to the purpose for which it is used. Annington must not collect Personal Data that is simply convenient or "nice to have", which is not **necessary** for the processing purpose(s) for which the individual has provided his/her Personal Data, or which is to be used for another purpose (e.g. marketing) about which the individual has not been informed through Fair Notice. You should consider carefully how much Personal Data you actually need for the legitimate business purpose(s) you have identified for your processing activity. It should only be the minimum necessary for the purpose. **Information should only be collected for the purposes of which the individual has been made aware.**

3.6 Personal Data must be Accurate

We must keep Personal Data accurate – and every reasonable step must be taken to erase or rectify inaccurate Personal Data. The best way to ensure that Personal Data is accurate is to check this with the individual at the time it is collected. Some personal information collected may change from time to time, such as address and contact details, bank accounts, creditworthiness and employment circumstances. If Annington takes a decision based on inaccurate information or otherwise discloses information to the wrong address it is conceivable that this may cause some harm to the individual concerned, in breach of the obligations placed on Annington by the data protection legislation.

It is therefore important that, where necessary, information is kept up to date. Individuals whose Personal Data is being processed should be requested to inform Annington of any changes to the personal information they provided at regular intervals (each time you contact them and at least annually). If a large volume of personal information or number of individuals is likely to be affected, the Data Protection Lead will make the individuals aware that they need to review the personal information provided.

You must update Personal Data with all necessary changes as soon as you become aware that it is inaccurate or out of date, and ensure that the updates are made across all relevant records and systems.

You must ensure that you provide true, accurate and up to date details for Annington's records.

3.7 Annington cannot keep Personal Data Forever (Storage Limitation)

Annington must not keep Personal Data in a form which permits us to identify the individual concerned for longer than is necessary for the agreed or permitted purposes for which it is used. Even greater care needs to be taken to ensure that Special Personal Data is not retained for longer than is necessary. Annington can continue to retain details where needed for dealing with any legal proceedings involving Annington, where required to be retained for minimum periods by law, such as for tax records, or similar justifiable reasons. More information on the retention of Personal Data can be obtained from the Data Protection Lead.

The Data Protection Lead will review data retention at regular intervals. You must comply with any Annington data retention guidelines.

3.8 Personal Data must be Processed in Accordance with Individuals' Rights

Individuals have rights in relation to Personal Data processed about them. Under UK GDPR these rights change and expand and in some cases will depend on the basis on which Personal Data is used e.g. by consent, or to perform a contract, or where required by law. These include:

- **Right to information** – See paragraph 3.2;

- **Right of access** – Individuals are entitled to receive confirmation from us as to whether or not we are processing Personal Data about them and, if we are, to access it and be provided with certain information in relation to it, such as the purpose(s) for which it is processed, the persons to whom it is disclosed and the period for which it will be stored;

- **Right to rectification** – Individuals can require us to correct any inaccuracies without undue delay;

- **Right to erasure** (also known as the right to be forgotten) – Individuals can require us to erase their Personal Data, without undue delay, if we no longer need it for the purpose for which we have it or if it is being unlawfully processed or if erasure is required to comply with a legal obligation to which we are subject. There are some exceptions to this right;

- **Right to restriction of processing** – Individuals can require us to restrict processing in certain circumstances including if the Personal Data is inaccurate or if the processing is unlawful;

- **Right to data portability** – Individuals can, in certain circumstances, receive the Personal Data in a structured, commonly used and machine-readable format so that it can be transferred to another provider; and

- **Right to object** – Individuals can object to:

    - our processing of their personal data for direct marketing purposes;

    - any decision we make which is based solely on "automated processing" (i.e. without any human involvement) (N.B. There are some limits and exceptions to this right); and

    - us processing their Personal Data where we are relying on the lawful basis that our processing is necessary for a legitimate interest.

- **Right to withdraw consent** – Individuals have the right to withdraw their consent to our processing of their Personal Data at any time. If this happens, we must stop processing their Personal Data unless there is another lawful basis we can rely on – in which case, we must let the individual know (N.B. If someone withdraws their consent, it won't impact any of our processing up to that point).

You must ensure you are aware of more detailed Annington guidance on individual rights, how to recognise them and how to respond to requests.

An individual must not have their credit worthiness checked (or any Personal Data about them passed to credit reference agencies) except with the prior consent of that individual in circumstances agreed in advance by the Data Protection Lead.

If you receive any communication from an individual in relation to their Personal Data or from any other person or body (including the Information Commissioner's Office) in relation to Personal Data, you must inform the Data Protection Lead immediately, and provide details of the relevant communication.

We have to respond to certain requests from individuals in relation to their Personal Data within strict timescales, so it is very important that the Data Protection Lead is made aware of each request **as quickly as possible**. You must also cooperate with the Data Protection Lead by providing any other information and assistance that they may require.

Please do not, under any circumstances, respond to requests or communications about Personal Data yourself without input from the Data Protection Lead.

3.9 Appropriate Security must be Applied to all Personal Data (Integrity and Confidentiality)

Annington must have appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing and accidental or unlawful destruction, damage loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise processed. We may have to report any threat to or breach of security to the Information Commissioner's Office within 72 hours of

becoming aware of the breach and to any affected individuals (whose Personal Data is involved). Further details of reporting requirements can be found in Annington's Personal Data Breach Policy.

Special security measures will be required to be put in place in the case of Special Personal Data, bank account details or similar confidential material which may cause damage or distress if lost or misused. Further details can be found in Annington's User Policy for Information Security.

We need everyone's help to keep Personal Data secure and everyone shares responsibility for this. You should help us do this by:

- complying with our IT and information security policies documented in the User Policy for Information Security and our Employee Handbook;
- considering carefully what format (e.g. paper or electronic) is required for the Personal Data you are processing;
- using common-sense, practical measures to protect the security of Personal Data (and in particular Special Personal Data), for example:
    - if you need to use paper records ensure that they are locked away/stored in secure filing cabinets when not in use and dispose of them in confidential shredding bins once they are no longer required;
    - do not leave printing containing Personal Data on printers;
    - lock your screen when you are away from your desk;
    - never share passwords or login details with others; and
    - ensure that others cannot read the information on your screen over your shoulder.
- before sending an email – pausing and checking that the content, attachments/enclosures and addresses/recipients are correct and that the email will be sent only to the people it's intended for, and if appropriate that any data is encrypted;
- not sharing Personal Data with anybody (including people within our business) unless you are sure who they are and why they need access to the relevant Personal Data; and
- ensuring the ongoing confidentiality, integrity, availability and resilience of the processing systems and services we use for processing Personal Data.

Third parties (i.e. companies, businesses or people outside Annington Limited (including other Annington Group entities)) may need to access the Personal Data we process, for example as part of providing services to us. However, we are only permitted to disclose Personal Data to third parties in certain limited circumstances. Third parties who process Personal Data on behalf of Annington (known as a data processor) must sign an appropriately worded data processing contract to ensure compliance with the data protection legislation. Examples of data processors are external payroll providers, outsourced records archiving providers or shredding service providers. UK GDPR contains mandatory wording to be included in contracts.

When we are considering engaging a supplier outside of Annington Property Limited to process Personal Data on our behalf (a "**third party supplier**"), we must always have regard to the following:

- Due diligence - we must select a third party service provider who provides sufficient guarantees with respect to data security and the handling of Personal Data generally.
- Contractual obligations - we must ensure that there is a written contract in place with the third party service provider which includes specific data privacy obligations protecting Personal Data. Therefore, always check with the Data Protection Lead before sharing any Personal Data with a third party service provider.
- Compliance monitoring - we must take reasonable steps to monitor the third party service provider's performance of the relevant security and processing obligations.

- International transfers - if engaging a third party service provider will or may involve Personal Data being processed abroad or overseas, additional data protection and privacy considerations must be addressed and this generally means that additional clauses must be included in the contract (see paragraph 3.10 below).

As discussed above, appropriate due diligence will be required in advance on such providers to ensure they are suitably secure and reliable. Suitable due diligence checklists and contract wording is available from the Data Protection Lead. You must not use or agree to other forms of wording without prior written approval from the Data Protection Lead.

We must never disclose Personal Data outside Annington to anyone other than a third party supplier (see above) except where this is lawful (including where it is necessary):

- to protect an individual's vital interests;
- to comply with a law, regulation or court order, for example, where requested by customs officials for the investigation of tax offences;
- to respond to any legitimate request for assistance by the police or other law enforcement agency;
- to engage and/or obtain advice from professional advisers (e.g. accountants, lawyers, external auditors etc.);
- to deal with any legal dispute or administrative claim between us and a third party (e.g. to that third party and lawyers representing them);
- to liaise with potential overseas buyers or other third parties in connection with the disposal of or merging of any Annington asset(s) or entity/(ies); or
- as otherwise permitted by, and in accordance with, applicable laws.

You should always check with the Data Protection Lead if you are unsure whether or not you are permitted to disclose Personal Data to a third party.

Any disclosures to third parties should be approved by the Data Protection Lead in advance.

Personal Data must only be provided, disclosed and/or transferred to those with a business need (and suitable authorisation, where required) to access/receive it. You must not access or use more Personal Data than you properly need to know to carry out your role. You must not try to access or use Personal Data which you are not authorised to see or use. You must not misuse Personal Data, for example by using the data for your own purposes, or those of family or friends, or disclosing it to others to use for their purposes. This would be a breach of our data security rules. It could be a breach of applicable data protection laws and indeed be a criminal offence in some cases.

A "**Personal Data Breach**" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. It covers malicious incidents such as a cyber-attack, but it also covers other incidents many of which can arise as a result of human error. For example, a lost laptop, device or file or giving Personal Data to the wrong person over the telephone or via email.

Under UK GDPR, Annington must record all Personal Data Breaches affecting it and its Personal Data. In many cases, Annington will be obliged by law to inform the regulator of such breaches **within 72 hours** and may also need to inform affected individuals. If you discover or suspect that there is or has been a Personal Data Breach, you must inform the Data Protection Lead **immediately** using the email address dataprotection@annington.co.uk by telephone on 07468 495 662. It is important that you do this immediately as we are required by law to deal with Personal Data Breaches within very strict timescales. These are not limited to 9am-5pm Monday to Friday. You must ensure that you are aware of and comply with Annington's Personal Data Breach Policy in respect of data security and dealing with Personal Data Breaches.

Under no circumstances must Personal Data be released about an individual to any person requesting this information by phone, fax or post, unless the identity of the person making the request and that they are entitled to receive the information requested has been confirmed. Please note that as a general rule parents,

spouses, partners and children are not entitled to information about their relatives. Please liaise with the Data Protection Lead in this case.

3.10 Transfers outside the United Kingdom

Annington will not transfer personal information outside the United Kingdom (UK) unless:

- it has first obtained consent from the individual;
- the transfer is to a country which has been deemed adequate by the UK Government); or
- necessary steps have been taken to ensure that the information transferred is kept secure.

A transfer includes remote onscreen access from outside the UK to personal details still stored on servers in the UK.

The countries currently deemed adequate include EU Member States and institutions, European Economic Area member states, Andorra, Argentina, the Faroe Islands, Guernsey, Jersey, Isle of Man, Switzerland, Canada (in certain circumstances), Gibraltar, Israel, Japan (in certain circumstances), Uruguay and New Zealand.

All transfers of personal information outside the UK must be approved first by the Data Protection Lead as additional contractual measures to ensure adequate safeguards for the Personal Data being provided may be required by law and Annington must keep records of all such transfers and why they are adequately safeguarded. The UK now has its own forms of standard contractual clauses which should be used for affected data transfers to outside the UK and it is no longer possible to use only the EU's form of standard contractual clauses for them.

3.11 Direct marketing and sale of Personal Data

There are strict laws which govern direct marketing practices (in addition to data protection legislation). Annington must not send direct marketing communications to any individuals (including business partnerships) unless it complies with complex rules about that use and the means of communication. Where the direct marketing may be by email or other electronic means, explicit consent to that type of contact must also be obtained in advance. This consent can be obtained at the time Personal Data is collected from or provided by an individual, following provision of the relevant Fair Notice. Such consents can be withdrawn by the individual at any time and must be dealt with promptly by Annington. Consents used must be the appropriate Annington approved form of consent.

All electronic direct marketing communications sent must provide a link which provides the recipient with a simple means of unsubscribing from (or 'opting out' of) future communications of this type, should they wish to. Other marketing communications must also contain appropriate information to help individuals to easily unsubscribe from direct marketing, in whole or part.

Annington must comply with any request by an individual not to receive direct marketing information.

Additionally, the Telephone, Fax and Mail Preference Services must be checked prior to marketing to any individual by those means. As with electronic marketing we must always provide individuals with a simple means of unsubscribing from (or opting out of) our marketing communications, in every communication we send. Elections not to receive marketing by such means must be complied with.

Should you have any queries about whether direct marketing can or cannot be undertaken, please contact the Data Protection Lead.

5 Conclusion

Annington has a legal obligation ensure that Personal Data is processed in accordance with data protection legislation and principles. Annington cannot comply with its legal obligations unless all employees and all relevant contractors ensure that they comply with Annington's Policy.

Data Protection helps prevent serious crime and reputational damage. Our policies are there to protect prospective, former, future and current customers as well as our employees and contractors. Failure to comply could be regarded as a serious breach of employment or other contractual terms and employees and Directors of Annington may also face personal liability and criminal liability in certain circumstances.