

ALLSAINTS

General Data Protection Regulation (GDPR)

Privacy Notice for Candidate Applications / Recruitment Purposes

AllSaints is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you at the point of applying for a position with AllSaints in accordance with the General Data Protection Regulation (GDPR).

Contents

Welcome.....	2
Overview	2
Definitions	2
Data Protection Principles	2
What Information do we hold about you?	3
How is your Personal Data collected?	3
How we will use information collected?	4
How we use Sensitive Personal Information	5
Automated Decision Making.....	6
Data Sharing	6
Data Security	7
Data Retention.....	8
Rights of Access & Erasure.....	8
Subject Access Requests	9
Right to Withdraw Consent	9
Further Information	10
Policy status.....	10
Annex 1: Examples of Personal Data Use.....	11
Document History	12

ALLSAINTS

Welcome

We want you to be confident we'll protect your personal information and respect your privacy. This policy explains how we use your personal information - what information we collect about you (including from third parties), why we collect it, what we do with it and on what basis.

Please read it carefully. It applies to personal information we collect during the recruitment process. Please contact the People and Culture team if you require the privacy notice applicable to employees, contractors and workers during & after employment.

We have included a definitions section in this document which explains the meaning of any technical terms we use.

Overview

AllSaints is a "data controller" which means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to applicants, candidates and prospective employees or prospective workers across the UK and EU. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

Definitions

- General Data Protection Regulation (**GDPR**)
- "**Personal data**", or personal information: means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are "special categories" of more sensitive personal data which require a higher level of protection.
- Data Protection Act 1998 (**DPA**)
- "**Third parties**" includes third-party service providers (including contractors and designated agents) and other entities within our group
- "**Data subject access request**" Request access to your personal information that is held by the Organization
- **Anonymised data** means data which has had all personally identifiable information removed.

Data Protection Principles

We will comply with General Data Protection Regulation (GDPR) and Data Protection Act 1998 (DPA). This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that

ALLSAINTS

is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

What Information do we hold about you?

We will collect, store, and use the following categories of personal information about you:

- Personal contact details
 - a. name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth
- Copy of birth certificate
- Gender
- Nationality
- Marital status and dependents
- Next of kin and emergency contact information
- National Insurance number
- Bank account details, payroll records and tax status information
- Employment history
 - a. Salary, annual leave, pension and benefits information
 - b. Education and training records, certificates
- Copy of driving licence
- Copy of passport and any other right to work documents such as a visa or national identity card
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).

We may also collect, store and use the following “special categories” of more sensitive personal information:

- Information about your health, including any medical conditions
- Health records (such as doctors notes) you have shared with us
- Biometric Residence Permits

How is your Personal Data collected?

We collect personal information through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes

ALLSAINTS

collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

We will collect additional personal information during your employment via job-related activities throughout the period of you working for us.

How we will use information collected?

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest (or for official purposes)
- When requested to do so from any government body for legal matters

Situations in which we will use your personal information

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations.

- Provide you with health and safety support at work. This includes work related injuries, illness, management of your health and safety, providing any accessibility support you may need (including where you make us aware in your health declaration on joining us and as updated by you when appropriate) and contacting your emergency contact if ever needed. This may include us making a referral to the occupational health service.
- Further information about you. This may include your information relating to your health, nationality, race, religion, ethnic origin, preferred language, sexual orientation details of any accessibility requirements you have, criminal offences (more details below), proceedings and/or convictions and anything which would restrict your ability to work, and for us to comply with equality and diversity requirements as an employer.
- Use information as needed to prevent and detect unlawful activity. This may include the use of biometric information such as retina scans and fingerprints for secure building access.
- Compile and manage our case in a legal claim made by or against us. Such processing is subject to strict confidentiality provisions.
- Offer you the chance to join a share plan if you are eligible to join.

In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests.

We'll use your personal information where we have a legitimate interest in doing so to promote and protect our business.

ALLSAINTS

Examples of situations in which we will process your personal information are listed in Annex 1 in this document. We have indicated the purpose or purposes for which we are processing or will process your personal information, as well as indicating which categories of data are involved.

Some of the above grounds for processing will overlap, Annex 1 is not exhaustive and is subject to change in accordance with new requirements legally. There may be several other circumstances which justify our use of your personal information.

We'll keep some of your personal information for the following purposes:

- Your contact details and anything needed to verify who you are. This includes your name, address, phone numbers, date of birth, email address, CV data.
- Further information about you. This includes your gender, nationality, race, ethnic origin, religion, sexual orientation, preferred language, health and details of any accessibility requirements you have, for application progress
- Information about your application history

If you fail to provide personal information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

Change of purpose

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How we use Sensitive Personal Information

“Special categories” of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:

- In limited circumstances, with your explicit written consent.
- Where we need to carry out our legal obligations and in line with our Privacy Standard.
- Where it is needed in the public interest, such as for equal opportunities monitoring, or in relation to our occupational pension scheme, and in line with our Privacy Standard.
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the

ALLSAINTS

appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

Do we need your consent?

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Automated Decision Making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. We are permitted to use automated decision-making in the following circumstances:

- Where we have notified you of the decision and given you 21 days to request a reconsideration.
- Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.
- In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal information, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

Data Sharing

We may have to share your data with third parties, including third-party service providers and other entities in the group. We require third parties to respect the security of your data and to treat it in accordance with the law. We may transfer your personal information outside the EU. If we do, you can expect a similar degree of protection in respect of your personal information.

Why might you share my personal information with third parties?

ALLSAINTS

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

Which third-party service providers process my personal information?

“Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, IT services, visa advisors, travel partner and other types of carefully selected 3rd party providers.

How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Legal Disclosures

We may at times be required to disclose personal information about you to law enforcement agencies. The law enforcement agencies may ask for disclosure of one or more of the following items of personal information:

- Your contact details or information to validate your identity.
- Your payment and financial information.
- Information about your time with us.
- Records of your use of communications services and activities.

We disclose personal information to law enforcement agencies so they can detect and stop crime, prosecute offenders and protect national security. We only share your personal information in accordance with applicable law, we have strong internal oversight of what we do and we take expert advice to inform our approach.

We may also share personal information about you where we are under a legal obligation to disclose it to another person. These obligations arise because of a law that obliges us to disclose that information or because of a court order requiring disclosure of that information.

We may also disclose information to a public authority. We only do this where they have provided assurance and we have assessed that their request is proportionate and necessary. For example, the disclosure of information to the Department of Work and Pensions in benefit cases.

Data Security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. Details of these measures are available upon request.

In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

ALLSAINTS

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data Retention

How long will you use my information for?

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

We keep recruitment information for 12 months should you reapply for another position becomes available you might be interested in (you can tell us if you don't want to be contacted).

Rights of Access & Erasure

It is your duty to inform us of any changes to your personal information.

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- Request the transfer of your personal information to another party.
- If you want to review, verify, correct or request erasure of your personal information, object to the

ALLSAINTS

processing of your personal data, or request that we transfer a copy of your personal information to another party, please speak to your line manager.

Erasure / Changes

When you delete or change (or ask us to delete or change) your personal information from our systems, we might not do so straight away from our backup systems or residual copies on our active servers. And we may need to keep some information to fulfil your request (for example, keeping your email address to make sure it's not on a marketing list).

If you do not provide your personal information, provide it inaccurately or require us to delete it, then we may not be able to provide you with a contract for employment or carry out our obligations, such as paying you. It may also prevent us complying with our legal obligations, like paying your tax.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Subject Access Requests

Data subjects may make a request for disclosure of their personal information. A data subject access request is subject to the statutory conditions from time to time in place and should be made in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

In order for us to comply with your request please provide as much information as possible. We will comply with any such requests within 1 month, however at times may extend this timeframe to 3 months in accordance with the ICO time frames.

We can decline if we believe doing so would adversely affect others or the law stops us. And even though we have to complete your request free of charge, we are allowed to reject requests if they're repetitive, you don't have the right to ask for it or the requests made are excessive. If that's the case, we'll explain why we believe we don't have to fulfil the request.

To make a data subject access request you should either contact HR@allsaints.com or gdpr-submissions@allsaints.com, detailing the full details of your request.

Right to Withdraw Consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Your withdrawal of consent only applies to how we use your personal information in the future, not what we've done in the past

Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

To withdraw your consent, please contact the people and culture team.

ALLSAINTS

Further Information

If you are not satisfied with the handling of your data, also have a right to lodge a complaint with supervisory authority by writing to the Information Commissioner's Office <https://ico.org.uk/concerns/handling/>

This notice doesn't apply to the information we hold about companies or other organisations. The notice is intended to tell you how we use personal information but is not intended to create a contract with you. This notice doesn't apply to other companies or organisations collecting and using your personal information. You should review their privacy policies before giving them your personal information.

Policy status

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact People and Culture hr@allsaints.com.

ALLSAINTS

Annex 1: Examples of Personal Data Use

The purpose	Categories of personal data
Making a decision about your recruitment or appointment	CV, references, name, address, email address, phone number
Determining the terms on which you work for us	CV, references, certificates, educational and training records
Checking you are legally entitled to work in the UK	Copy of the passport, visa, right to work
Paying you and, if you are an employee, deducting tax and National Insurance contributions	Bank details, National Insurance number, name, address, email address, date of birth, marital status, salary and benefits details
Providing the following benefits to you: pension, childcare vouchers, cycle to work scheme, healthcare	Name, address, number of dependants, email address, phone number
Liaising with your pension provider	Name, address, date of birth, salary details, email address
Administering the contract, we have entered into with you	Name, Contact details, Date of birth, Birth Certificate, Marital status, Gender, Nationality, Health details, C.V., Bank Details Identity Documents, References, Leave (annual, sickness), Education & training information/ certificates, Visa/work permit/BRP, next to kin (emergency contact)
Equal opportunities monitoring	Gender, age, nationality, ethnicity, medical history

ALLSAINTS

Document History

Version Number	Date of issue	Summary of changes	Issued by
V 1	22/06/2020	Update	Sophey Layton