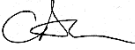


September 2024



# DATA PROTECTION POLICY

Issue date: September 2024

Signed: 

Review period: Annually

DATA PROTECTION POLICY ISSUES AND UPDATES

PAGES	ISSUE	DATE
ALL	Review of whole policy and re-issue	22/07/2024

The following policy has been approved by the Senior Leadership Team and the Board of Trustees.

The policy will be reviewed on an annual basis unless circumstances arise requiring the policy to be reviewed earlier.

Approved by Board of Trustees: July 24.

Board signatory: Jon Drown

Planned review: July 2025

## CONTENTS

<a href="#">1.Introduction</a>	Page 4
<a href="#">2.Aims of the policy</a>	Page 4

<a href="#">3.What does the law say?</a>	Page 4
- <a href="#">What is GDPR?</a>	Page 4
- <a href="#">What is personal data</a>	Page 4
- <a href="#">What is sensitive personal data?</a>	Page 5
- <a href="#">Examples of personal data and sensitive personal data</a>	Page 5
- <a href="#">Who regulates the GDPR in the UK?</a>	Page 5
- <a href="#">What happens if we get it wrong?</a>	Page 5
- <a href="#">The 8 data protection principles</a>	Page 5
1) <a href="#">Fairly, lawful and transparent</a>	Page 5
2) <a href="#">Use it only for a limited purpose</a>	Page 5
3) <a href="#">Data Minimisation</a>	Page 6
4) <a href="#">Accuracy</a>	Page 6
5) <a href="#">Data retention</a>	Page 6
6) <a href="#">Respecting the individual's legal rights</a>	Page 6
7) <a href="#">The security (or 'ATOM') principle</a>	Page 6
8) <a href="#">Don't let personal data leave the UK without telling us</a>	Page 6
3.7 <a href="#">Accountability</a>	Page 6
<a href="#">4.Who can I speak to about data protection issues at Saints?</a>	Page 7
<a href="#">5.Taking Ownership</a>	Page 7
<a href="#">6. New Ideas</a>	Page 7
<a href="#">7. Data Breaches</a>	Page 7
<a href="#">8. Sharing information with other organisations</a>	Page 7
<a href="#">9. Dealing with subject access requests</a>	Page 7
<a href="#">10. Right to be forgotten requests</a>	Page 8
<a href="#">11. Changes to this policy</a>	Page 8

## DATA PROTECTION POLICY

### 1 INTRODUCTION

This Data Protection Policy sets out the roles, responsibilities and procedures around the use of personal data within Northampton Saints Foundation (“**Foundation**”). This policy applies whenever you are collecting or handling personal data in any way.

Everyone has rights about the way in which their personal data is handled. During our activities we will collect, store, and use personal data about customers, our fellow colleagues and our suppliers, we will also be asked to share personal data with authorities.

Any breach of this policy may result in disciplinary action by the Foundation in accordance with Foundations’ disciplinary policy. This policy does not form part of any employee's contract of employment and may be amended at any time.

## 2. AIMS OF THIS POLICY

1. To outline the framework of rules around collecting, handling, using, transferring and storing personal data.
2. To protect the rights and freedoms of individuals in relation to the use of personal data within the Foundation.
3. To help you understand the fundamentals of data protection law.
4. To guide you to help ensure that the Foundation is compliant with data protection laws.
5. To understand the risks to the Foundation of non-compliance with data protection laws.

## 3. WHAT DOES THE REGULATION SAY?

### 3.1 What is GDPR?

The General Data Protection Regulation (“**GDPR**”) is an EU Regulation and is the biggest change to data protection law in 20 years and it came into force on 25 May 2018, replacing the Data Protection Act 1998 (“**DPA**”). The UK on leaving the EU wrote a copy of GDPR into its statute book and it became known as UK GDPR and it currently copies the EU version GDPR. The aim of the new regulation is to give individuals new rights over their data. These include eight rights on what you can do with your data and the type of privacy you can expect from companies who hold your data.

### 3.2 What is personal data?

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

Examples of personal data are set out in the table below. If you are unsure about whether certain information is personal data or not, please speak with our DPO (please see paragraph 0 of this policy for contact details of the DPO).

Controller or Processor - Controllers are the main decision-makers – they exercise overall control over the purposes and means of the processing of personal data.

If two or more controllers jointly determine the purposes and means of the processing of the same personal data, they are joint controllers. However, they are not joint controllers if they are processing the same data for different purposes.

Processors act on behalf of, and only on the instructions of, the relevant controller.

### 3.3 What is sensitive personal data?

It's not just that this type of information might be seen as more sensitive or 'private'. The recitals to the UK GDPR explain that these types of personal data merit specific protection. This is because use of this data could create significant risks to the individual's fundamental rights and freedoms. For example, the various categories are closely linked with:

- freedom of thought, conscience and religion;
- freedom of expression;
- freedom of assembly and association;
- the right to bodily integrity;
- the right to respect for private and family life; or
- freedom from discrimination

#### Examples of personal data and sensitive personal data

Please note that the categories in this list are examples and this is not an exhaustive list:

Personal Data	Sensitive Personal Data
Name (first name or second name)	Religious expression
Age	Physical or mental condition
Address	Political views and beliefs
Phone number	Racial or ethnic origin
Email address	Criminal record checks
Photograph	Trade union membership
Location	Sex life
Opinion	Sexual orientation
Bank details	Biometric data (e.g. information obtained from fingerprint or retina scanning)
Salary	
Opinion	
Bank details	

### 3.4 Who regulates the GDPR in the UK?

In the UK, the Data Protection regulations are independently enforced by the Information Commissioner's Officer ("ICO") Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF. Telephone: 0303 123 1113,. The current commissioner is John Edwards.

### 3.5 What happens if we get it wrong?

The ICO has a wide range of powers. It can issue an enforcement notice where it requires a business to remedy a certain breach. It can also publicise data protection breaches on its website which could lead to negative publicity for the Foundation. It also has the right to audit Northampton Saints Foundation and fine the Foundation up to €20 million or 4% of global turnover for serious breaches of the Data Protection Laws. However, in reality the ICO does not take the fining of charities as productive and would prefer to be them on remand and work with the charity to resolve the issue.

### 3.6 The 8 data protection principles

The DPA sets out 8 data protection principles which you should be aiming to follow at all times. The GDPR condenses this to 6 principles but, in practice, it does not change the substance of the 8 principles under the DPA. They are as follows:

- (1) **Fairly, lawful and transparent.** - The first principle is that personal data shall be processed fairly, lawfully and transparently. The Data Protection Laws are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individuals whose data you are using.
- (2) **Use it only for a limited purpose** - The second principle is that personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. Whilst at the Foundation, you may be collecting personal data in different ways. This may include data you receive directly from individuals and data you receive from other sources. You must not use the data for your own personal purposes and instead it should be used strictly as part of your employment only.
- (3) **Data minimisation** - The third principle is that personal data shall be adequate, relevant and limited to what is necessary. You should only collect, use, access or analyse personal data to the extent that you need to. You should ask yourself: am I doing the minimum amount necessary with personal data to achieve my purpose?
- (4) **Accuracy** - The fourth principle is that personal data shall be accurate and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of-date data.
- (5) **Data retention** - The fifth principle is that personal data shall be kept for no longer than is necessary. The Data Protection Laws do not tell us how long is necessary. We therefore have a separate Data Protection Retention Policy to guide you in determining how long to keep certain types of information. Please refer to the policy for your department for further details about how long you should be keeping certain types of personal data and how you should be deleting personal data. The Data Retention Policy for your department can be obtained from the DPO or from your line manager.
- (6) **Respecting the individual's legal rights** - The sixth principle is that personal data shall be processed in accordance with the rights of data subjects (i.e. the individuals about whom Northampton Saints Foundation are using personal data). Please see paragraphs 9 and 10 for further detail about individuals' right of access to the information The Foundation hold about them (commonly known as a subject access request or "SAR") and their right for information about them to be erased (typically referred to as the "right to be forgotten").

- (7) **The security (or “ATOM”) principle** - The seventh principle is that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage. The GDPR says that we must use “appropriate, technical and organisational measures” to keep data secure.

*Security of personal data applies to a range of areas, including IT security, and it particularly should be applied throughout your day-to-day activities. For example, are you copying the correct email addresses into a particularly sensitive email? Is it more appropriate to use the blind carbon copy function (i.e. Bcc)? Are all of your belongings (e.g. laptops, notebooks) kept securely?*

(8) **Don't let personal data leave the UK without telling us** - The final principle is that personal data must not leave the European Economic Area unless certain legal protections are in place. If you would like further details about this principle or have any queries, please speak to the DPO (please see paragraph 3.7 below). Otherwise, if you are aware of personal data being transmitted outside of the UK (for example, you might be using an application provided by a company with servers storing personal data in, say, India), you must tell the DPO immediately. This might mean having to do some investigation as to how personal data flows in and out of the organisation.

### 3.7 Accountability

The GDPR also introduces the principle of accountability. In other words, you must be able to demonstrate the 8 data protection principles and you need to take ownership and responsibility of them for yourself. This is normally demonstrated through an accountability audit provided by the DPO annually.

## 4 WHO CAN I SPEAK TO ABOUT DATA PROTECTION ISSUES AT SAINTS FOUNDATION?

The Saints Foundation have appointed a Data Protection Officer (“DPO”) who is responsible for overseeing compliance with the Data Protection Laws and with this policy. That post is held by Catherine Deans, Northampton Saints Foundation Managing Director. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

## 5 TAKING OWNERSHIP

The GDPR introduces a new requirement called data protection by “**design and default**”. It essentially means that we all have a responsibility to proactively build the 8 principles (set out in paragraph 3.6 above) into our everyday systems, business processes and activities.

## 6 NEW IDEAS

You may want to introduce something new and innovative to the organisation. It is important that, before implementing anything new, you speak with the DPO. Under the new concept of data protection by design and default (please see paragraph 5), we will need to ensure that we have built good data protection practice into any new idea before implementing the idea. Sometimes, this will require a formal data protection impact assessment where the new idea is potentially high risk to the privacy customers and/or members of staff.

## 7 DATA BREACHES

A personal data security breach is any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It could be as a result of a cyber-crime. Or it could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission. It may be accidentally sending an email attachment to the wrong person. It could be leaving confidential information about a person or group of people exposed in a public place or left on public transport. It could even be losing your laptop, device or notes.

Whatever the issue is, you need to tell the DPO about it immediately and seek all the background details (i.e. when and how it happened and who has been affected). GDPR requires the Foundation to report personal data breaches to the regulator within 72 hours of first becoming aware of it if the level of risk to those individuals is high, if we decide it is of low risk we do not have to advise the ICO. **Please do not report the breach to the ICO yourself. If in doubt, contact the DPO.**

## 8 SHARING INFORMATION WITH OTHER ORGANISATIONS

If you are looking at engaging with any new school/customer, and you know that the school/customer will be obtaining personal data relating to the Foundations' members of staff or other groups of people, you must complete a data sharing agreement form in advance of any data sharing.

The GDPR requires the Foundation to (a) vet these suppliers to ensure that they offer an appropriate level of security of personal data and (b) make sure that there is a written contract between the supplier and the Foundation and that this written contract is GDPR-compliant before being signed.

## 9 DEALING WITH SUBJECT ACCESS REQUESTS

A subject access request (“**SAR**”) is a written request from an individual to obtain a copy of the information the Foundation holds about him or her. This is a statutory right; however, it is not without its complications, and it doesn't just mean disclosing every piece of information because there might be legal or commercial reasons to withhold certain information, this also includes CCTV. The individual issuing a SAR could be a customer, member of staff or member of the public. A SAR only needs to be made in writing to be valid and does not require any other formalities (for example, it does not need to be addressed to any particular person at the Foundation and it can be made by email, post, fax, text or possibly even social media).

As there are strict time periods for complying with a SAR (one calendar month from the date of the SAR), it is important that you immediately notify the DPO who will then provide all necessary assistance. **Please do not respond to the individual without first consulting the DPO.**

## 10 RIGHT TO BE FORGOTTEN REQUESTS

A “right to be forgotten” or erasure request is a request from an individual to have information which the Foundation holds about him or her erased. Like SARs, this is a statutory right but not as straightforward as you might think, and it doesn't just mean deleting every piece of information about the individual because there might be legal or commercial reasons to keep certain information. As with SARs, please make sure that you contact the DPO immediately



before responding to the individual making the request. **Please do not respond to the individual without first consulting the DPO.**

## 11 CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where the changes are significant, we will make sure that we tell you about them.