



St Mary's Football Group Limited

Privacy & Data Protection Policy

February 2019



INTRODUCTION

St Mary's Football Group ("SMFG") holds a large amount of personal data. This relates to job applicants, players, academy scholars, host families, our employees, sponsors, suppliers, fans and many other individuals.

We use this information for a variety of business purposes. This policy sets out how SMFG seeks to protect personal data and ensure our staff understand the rules governing their use of personal information to which they have access as part of their work.

As we seek to engage more actively with our fans and business partners, we must continue to be seen as an organisation that people can trust with their personal data, particularly as we hold a lot of personal data which is sensitive in nature. This sensitive data relates to our playing staff, academy players and other employees.

WHO DOES THIS POLICY APPLY TO?

This policy applies to all companies in the St Mary's Football Group, as well as any other affiliated companies and organisations. Currently, this includes

- St Mary's Football Group Limited;
- All actively trading subsidiary companies of SMFG namely Southampton Football Club Limited, St Mary's Catering Limited and St Mary's Training Centre Limited; and
- All affiliated organisations such as Saints Foundation.

This policy also applies to the global transfer or receipt of data. If you want to transfer data outside of the UK, the standard within this policy applies. Anyone wanting to transfer or receive data from a company outside of the UK must contact the Legal department.

This policy requires all staff to ensure that they consult with the Legal department before starting any significant new data processing activity. This will help to ensure that all risks can be appropriately assessed and relevant compliance steps introduced at the earliest stage possible. Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct.

All staff must read, understand and follow this policy at all times.





OUR PRINCIPLES

Our policy is that we only process personal data in accordance with any applicable data protection laws and rights of individuals. Such laws and rights have been strengthened in the EU General Data Protection Regulation 2016/679 and the Data Protection Act 2018.

All staff are personally responsible for the practical application of this policy. Importantly, everyone must understand the need to consider the impact of any data protection regulations in countries outside of the UK where we have operations or are seeking to transfer data to. All staff are expected to completed mandatory data protection training within their first month of starting their employment with SMFG. For more information about the mandatory training, please contact the Legal department.

Everyone must observe the following principles in respect of the processing of personal data:

1. we will process personal information lawfully, fairly and in a transparent manner;
2. we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
3. we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
4. we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
5. we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
6. we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
7. we will never to transfer personal data without ensuring that adequate protection is in place. The safeguards required will be particularly robust when transferring any data outside of the European Economic Area.

WHAT IS PERSONAL DATA?

Personal Data

Is information that could be used to identify any living individual regardless of the form in which it is held. This includes all information held as a paper copy, electronically or digitally stored. This could be a single piece of information or multiple bits of information that could be pieced together to identify an individual.

Importantly, personal data includes any expression of opinion about any individual or any indication of our intentions towards an individual. All staff should keep this in mind at all times as it means that all opinions or intentions (including those set out in any notes or emails) may have to be handed over to an individual if they request it.

Special Category Personal Data

Is personal data that relates an individual's:

- racial or ethnic origin;
- political opinions;
- religious or similar beliefs;
- trade union membership;
- physical health;
- mental health;
- sexual life; and
- criminal record or any related proceedings.

Penalties for any misuse or mishandling of special category personal data (sometimes called "sensitive personal data") are more severe. All use, storage or transfer of any personal data must comply with this policy.



PROCESSING DATA FAIRLY

Collecting Personal Data

When gathering personal data or setting up new data processing or sharing activities, all staff must ensure that individuals whose data is to be processed know all of the following:

- Exactly what information about them we are collecting and want to process.
- All specific reasons and purposes for collecting and processing that information.
- Who any data will be disclosed to or shared with (this includes all group companies and any external parties).

Staff must make sure that personal data being collected and processed by them remains adequate, relevant and proportionate for the purpose for which it was obtained.

Processing Personal Data

Staff must not process any personal data unless:

- the individual whose details are being processed has provided clear and informed consent;
- the processing is necessary and legitimate to the performance of SMFG's legal obligations or to exercise our legal rights
- the processing is necessary for the performance of a contract to which the individual is party to in order to take steps at the request of the individual prior to entering into a contract;
- SMFG has a legitimate business interest in processing that data which does not prejudice the individual's privacy and we have the appropriate supporting documentation in place to support this; or
- the processing is necessary for the protection of the vital interests of the data subject or another natural person, usually only applicable if the processing will protect an individual's life.

Personal data obtained for one purpose must never be used for any additional or unconnected purpose without consent from the relevant individual

Special Category Personal Data

Unless otherwise advised by the Legal department, we must always obtain an individual's explicit consent to process any special category personal data relating to them. Prior to getting this consent, we must clearly explain to them exactly how we propose to use that information.

SMFG's data protection privacy notice sets out the types of special category personal information that we processes, what it is used for and the lawful basis for the processing. If you are unsure about the storage, transfer or processing of any special category personal data please contact the Legal department immediately.



DIRECT MARKETING

No one should ever make any contact with any individual to market any goods or services that we provide unless we have the express consent of that individual to do so. This includes all forms of marketing contact (e.g. email, by telephone). All staff must abide by any request from an individual not to use their personal data for direct marketing purposes. Everyone is responsible for ensuring that our lists of consent are maintained and accurate.

Staff should contact the Legal department for advice on direct marketing before starting any new direct marketing activity whether aimed at private individuals or commercial activities.

UPDATING INFORMATION

Everyone responsible for storing or processing any personal data must make sure that the information that they hold remains accurate and relevant to the purpose for which it was obtained.

This may mean that individual consent needs to be updated on a regular basis or the information itself needs to be reviewed or disposed of.



RETAINING DOCUMENTS AND INFORMATION

Personal data should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon a number of factors, including the reasons why the personal data was obtained. Staff must follow SMFG's document retention guidelines at all times.

Everyone must keep security issues in mind when disposing of information that they hold. All paper copies of personal information must be shredded or sent for secure shredding. Similarly, any electronic equipment must be appropriately wiped before being disposed of. Remember that deleting something from your computer does not permanently erase or destroy that information.

TRANSFERRING DATA SECURELY

No one must ever transfer any personal data outside of the UK without first consulting the Legal department. There are restrictions on international transfers of personal data from the UK to other countries because of the need to that ensure adequate safeguards are in place to protect the security of that information. Staff unsure of what arrangements need to be put in place should contact the Legal department before agreeing to transfer any data.

KEEPING INFORMATION SECURE

All staff must keep personal data secure against loss or misuse in accordance with SMFG's information security policies. Where SMFG engages any external organisation to process personal data on our behalf, appropriate security arrangements must always be implemented. Please involve the Legal department at the earliest opportunity so that any necessary steps to ensure compliance are addressed in the planning stages of any piece of work.

RIGHTS OF INDIVIDUALS

All individuals, including our staff, are entitled to request access to all personal information relating to them that we hold. Staff should never try to handle these requests themselves and they should always be referred immediately to the Legal department. This is particularly important because we have a legal obligation to respond to certain requests within a strict time limit.

Individuals also have the right to:

- be informed about how, why and on what basis their information is being processed as well as the right to correct inaccurate or incomplete data; and
- have their data erased if it is no longer necessary for the purpose of which it was originally collected or there is no longer a legitimate basis for processing the data (known as the right to be forgotten).

DATA BREACHES

A data breach may take many different forms. This includes the loss of data due to:

- theft of personal data or of equipment which personal information was stored on;
- the unauthorised access to or use of personal information either by a member of staff or third party;
- System failure (including hardware and software) whether due to hacking, viruses, phishing scams or unforeseen circumstances (such as flood or fire);
- human error (such as accidentally deletion or alteration of data);

Where SMFG suspects or considers that there has been a data breach, the Legal department will report to the Information Commission's Officer without undue delay and where possible, within 72 hours of becoming aware of the breach if the breach is likely to result in a risk to the rights and freedom of individuals. In such circumstances, we will also notify the affected individuals involved.

A member of staff is required to report their suspicion of any SMFG data breach as soon as possible to the Legal department in order to meet the required timeframe.

SPEAKING UP

All staff have an obligation to report any possible breaches of this policy. Anyone choosing to report a breach or any concern may raise this to their line manager, to the Legal department or using our external Speak Up channels. Reporting of any concerns at the earliest opportunity will allow us to fully investigate any possible failure and take appropriate remedial steps if any are necessary. It will also mean that we are able to submit any applicable notification within the relevant timeframe.

FURTHER INFORMATION

Anyone with any questions or concerns about this policy should discuss them with their line manager or the Legal department.

MONITORING & REVIEW

The Legal department is responsible for the monitoring and implementation of this policy. If you have any questions about the content of this policy, or any other comments, you should contact them at the earliest opportunity. This policy is subject to review at least once every two years although we may update it at any time. Any new or modified policy will be circulated to staff.



Never ignore any concern or leave it to others to report.

Always be responsible for *Speaking Up*.