Protecting Personal Data.

Guidance for all staff and volunteers

Author	John Cove
Role in Organisation	Director and Senior Safeguarding Manager
Date of Approval	January 2024
Date of Last Review	November 2025
Date of Next Review	November 2026

Personal data is the term used to describe personal information about an individual. It includes straight forward information like a person's name or age, and it includes more complex and sensitive data like a person's contact details, bank account details and shopping history. We need to collect personal data to manage relationships with our customers, staff and suppliers.

Personal data is incredibly valuable and to ensure it is not misused, it is protected by law. This means that we need to obey certain rules when handling data. It is easy to fall foul of these rules, which is why everyone in our group of companies must read and understand this guidance. There is a more technical version of this policy which provides guidance for people making decisions about how different pieces of data will be controlled.

This guidance explains what you need to think about when you:

- collect personal data
- keep personal data
- seek people's permission to use their personal data
- allow people to control the data we hold about them
- dispose of personal data
- manage mistakes and misuse of personal data.

This guidance does not cover all eventualities. If at any time you have any queries about your responsibilities or any aspect of data protection law, you must seek advice. Ryan Gawley is the Data Protection Officer (DPO) and will be able to provide you with the appropriate guidance.

Who is responsible for personal data?

If you collect or handle personal data, then you are responsible for making sure it is used appropriately. If personal data is misused, either deliberately or by mistake, then the company will be breaking the law.

What happens if something goes wrong?

If data is misused, lost or stolen, it is essential that this is reported immediately to the Data Protection Officer, via the email **dataprotection@stadiummk.com**.

All data breaches will be investigated and may lead to disciplinary action.

If you think that you have misused or lost data, it is important that you report this honestly and fully. Such action will be viewed positively when the breach is investigated.

The principles for maintaining and protecting personal data

The data protection laws set out 6 principles for maintaining and protecting personal data, which form the basis of the legislation. All personal data must be:

- processed lawfully, fairly and in a transparent manner and only if certain specified conditions are met;
- collected for specific, explicit and legitimate purposes, and not processed in any way incompatible with those
- purposes ("purpose limitation");
- adequate and relevant, and limited to what is necessary to the purposes for which it is processed ("data minimisation");
- accurate and where necessary kept up to date;
- kept for no longer than is necessary for the purpose ("storage limitation");
- processed in a manner that ensures appropriate security of the personal data using appropriate technical and
- organisational measures ("integrity and security").

What rights do people have when we hold their personal data?

Under data protection laws individuals have certain rights in relation to their own personal data. In summary these are the rights to;

- access their personal data, usually referred to as a subject access request;
- have their personal data corrected;
- have their personal data erased, usually referred to as the right to be forgotten;
- restrict processing of their personal data;
- object to receiving direct marketing materials;
- portability of their personal data;
- object to processing of their personal data; and
- not be subject to a decision made solely by automated data processing.

What does this mean for me?

If you need to collect, retain and use personal data, you must agree with your line manager the way that you will do this. Your line manager will discuss this with the Data Protection Officer before you collect any personal data. As part of the Stadium MK Group, you cannot just collect personal data without having an agreed system in place. This is so we can make sure we all collect data in a way which protects people's rights and is in line with the principles for maintaining and protecting personal data.

What does this mean for me?

- treat all personal data with respect
- treat all personal data how you would want your own personal data to be treated
- immediately notify your line manager or our DPO if any individual says or does anything which suggests they want to change the way we hold or use their data
- Take care to ensure all personal data and items containing personal data stay secure and are only available to authorised individuals
- immediately notify our DPO if you become aware of or suspect the loss of any personal data or any item containing personal data.

Some really practical tips for when using data?

Data protection laws are complex, but at the heart of the law is an expectation that organisations handle data carefully and responsibly. Handling personal data on a day-to-day basis is common-sense. The following list are some commonsense dos and don'ts.

Do not take or access personal data out of the organisation's premises or download personal data during remote access (unless absolutely necessary).

Keep passwords safe and secret (and change them if you need to share them with IT staff)

Never leave any items containing personal data unattended in a public place, e.g. on a train or in a café. This includes paper files, mobile phones, laptops and tablets.

Do not keep personal data on data sticks unless it is encrypted.

Never leave any items containing personal data in unsecure locations, e.g. in car on your drive overnight.

If you are staying at a hotel then utilise the room safe or the hotel staff to store items containing personal data when you do not need to have them with you.

Do encrypt laptops and other mobile devices containing personal data.

Do lock laptops, files, mobile devices and removable storage devices containing personal data away and out of sight when not in use.

Do password protect documents and databases containing personal data.

Take care when printing personal data on shared printers. Avoid printing whenever possible and make sure all personal data is collected when printing is complete.

Use confidential waste disposal or a shredder for any papers containing personal data; do not place these into the ordinary waste.

Do dispose of any materials containing personal data securely, whether the materials are paper based or electronic.

Be careful as to who might be able to see the information on your screen when you are working in public places. Ensure your screen faces away from prying eyes if you are processing personal data, even if you are working in the office.

Do challenge unexpected visitors or employees accessing personal data.

When speaking on the phone in a public place, take care not to use the full names of individuals or other identifying information, as you do not know who may overhear the conversation. Instead use initials or just first names to preserve confidentiality.

If taking down details or instructions from a customer in a public place when third parties may overhear, try to limit the information which may identify that person to others.

Never act on instructions from someone unless you are absolutely sure of their identity. If you are unsure then take steps to determine their identity.

Do not transfer personal data to any third party without prior written consent of our DPO.