

DATA PROTECTION POLICY



CONTEXT AND OVERVIEW

INTRODUCTION

We are committed to securing our customers' data to the highest degree. Worx Inductions needs to gather and use certain information about companies and individuals and can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact. That's why trust is the foundation of our privacy and data security promise to our customers.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

WHY THIS POLICY EXISTS

This data protection policy ensures Worx Inductions:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

DATA PROTECTION LAW

The Data Protection Act 1998 describes how organisations — including Worx Inductions— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- The head office of Worx Inductions
- All branches of Worx Inductions
- All staff and volunteers of Worx Inductions
- All contractors, suppliers and other people working on behalf of Worx Inductions

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- plus any other information relating to individuals

DATA PROTECTION RISKS

This policy helps to protect Worx Inductions from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

RESPONSIBILITIES

Everyone who works for or with Worx Inductions has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

GENERAL STAFF GUIDELINES

- All staff and contractors go through a vetting process and sign confidentiality agreements.
- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Worx Inductions will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from their direct manager if they are unsure about any aspect of data protection.
- We provide an ongoing program of security awareness education designed to keep all members of staff informed and vigilant of security risks.

PHYSICAL SECURITY

Worx Inductions's primary data centre is Global Switch, located in Sydney, Australia. With over 260,000 sq ft of property Global Switch is the largest data centre in the Southern Hemisphere. It offers a high quality, scalable solution with access to multiple carriers. The data centre's resilience is underpinned by a minimum N+1 standard for power and cooling systems, delivering an optimal operating environment to clients 24x7. The secondary data centre is in a separate offsite location in Alexandria, NSW Australia.

In addition, physical access is limited to a control list and mantraps with a dedicated security operations centre with 24x7 on-site security guards, constant CCTV surveillance and all areas are intruder resistant.

DATA STORAGE

- The entire Worx Induction application is encrypted with SSL.
- We use cookies for user authentication. We use session IDs to identify user connections. Those session IDs are contained in HTTPS-only cookies not available to JavaScript.
- Worx Inductions account passwords are one-way salted & hashed. Our own staff can't even view them. If you lose your password, it can't be retrieved — it must be reset.
- The databases are further protected by access restrictions, and key information (including your password) is encrypted when stored. Data is either uploaded directly into the application using a web browser or uploaded via the API which uses secure transfer protocols.
- All source code is industry best practices. We have separate environment and databases for different stages of application development. We do not use production data in our test and development environments.
- Servers are high end IBM database servers utilising SSDs and highly tuned MySQL software.
- Load balancers have been implemented, so as to not re-direct all traffic to one busy server.
- Back-up & redundancy are important which is why we utilise several layers of backup. Our NAS performs nightly snapshots which are used to provide fast access to data and this data is then replicated to our DR site in Alexandria. Weekly backups are performed on site to a separate device to provide a final layer of redundancy.
- With Network Attached Storage (NAS) there will be no delays when retrieving data from a local disk. There is also the added benefit that if a web server goes down, there is a greater level of redundancy, as all files are served on our NAS.
- Web clusters are used within the network, for safe and reliable server operation in case of an over load, the server is automatically removed from the pool minimising any effect on customers, as websites are dynamically distributed to other servers.

DATA USE

Personal data is of no value to Worx Inductions unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.

- Data must be encrypted before being transferred electronically.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data. It should be deleted and disposed of.
- Employees should request help from their direct manager if they are unsure about any aspect of data protection.

DATA ACCURACY

The law requires Worx Inductions to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Worx Inductions should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Worx Inductions will make it easy for data subjects to update the information Worx Inductions holds about them. For instance, via the company website.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by Worx Inductions are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, at privacy@worxinductions.com.au.

Individuals will be charged \$110 (inc gst) per subject access request. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Worx Inductions will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

PROVIDING INFORMATION

Worx Inductions aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. A version of this privacy statement will be available on the company's website when launched.

WORX
Inductions
ONLINE SAFETY MANAGEMENT

www.worxinductions.com.au