



Security and Privacy Policy

PRIVACY STATEMENT

Bright People Technologies ABN 26 098 142 744 (we, our) is covered by the Australian Privacy Principles (APPs), as set out in the *Privacy Act 1988* (Cth) (as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)). To comply with our obligations under the APPs, this Statement sets out how privacy is managed in our organisation and in particular, in Enable ERMS.

This Statement explains how we manage the personal information that we collect, use and disclose and how to contact us if you have any queries.

INFORMATION COLLECTION AND USE

Information on Authorised Users

Bright People Technologies owns and manages the ENABLE ERMS website, ENABLE ERMS software and databases, and related documentation.

The ENABLE ERMS System is used by Bright People Technologies clients (Asset Owner/s) to manage workforce policies, procedures and logistics on their Asset Sites. The Asset Owner nominates persons (Authorised Users) whom they wish to be given access to use the ENABLE ERMS System. Authorised users may be from the Asset Owner company and from companies to whom the Asset Owner has let contracts.

Authorised Users are given a unique user name and password to be used in accordance with "Terms and Conditions of Use of the ENABLE ERMS Website".

Information collected by Bright People Technologies on Authorised Users includes:

- Name and contact details of the Authorised User as provided on specific ENABLE ERMS System forms completed by the Authorised User or their employer;
- The time and date of each time the Authorised User logs in and logs out of the ENABLE ERMS System;
- A record of each time the Authorised User updates, inserts or deletes any record on the ENABLE ERMS System.

The above access and activity information is used to carry out effective administration and security management of the ENABLE ERMS system. Where required, it may be used to provide feedback to the relevant Asset Owner on Authorised User activity. It may also be disclosed to a third party engaged by Bright People Technologies for the purpose of system and network security, management and maintenance.

The ENABLE System does not use cookies to track any information on Authorised Users.

Information on Workers

A Contractor's Authorised User will submit information to the ENABLE ERMS system on individuals they are seeking to mobilise to an Asset Site (Worker/s). The information submitted is a subset of the information provided by the Worker on a Registration of Interest Form (ROI) form, as prescribed in the ENABLE ERMS System for the relevant Site. The subset of information is called a Request for Verification (RFV).

Worker information held on the ENABLE System includes:

- Name of the Contract company seeking to mobilise the Worker;
- Name of the Asset Owner and Site to which the Contract company is seeking to mobilise the Worker;
- Position to which the Contract company is seeking to mobilise the Worker;
- Name, date of birth, address, telephone contacts, and occupation of the Worker;



Security and Privacy Policy

The Worker's certificates, qualifications, licences and approval information (where supplied) and indication of eligibility to work in Australia;

- Persons nominated by the Worker to contact in the event of an emergency whilst engaged on the Asset site;
- Information supplied by the Worker to assess their match to the qualification requirements of the role. This may vary between Sites and clients but typically includes: occupations sought; education and other relevant qualifications; experience; employment history; workers' compensation history; indication of willingness to participate in fitness for work programs; name, company name and contact details of work history referees; and
- Health information supplied by the Worker regarding whether the Worker has a disability, injury, illness or condition which may affect their work performance, or may be aggravated by the type of work they apply for.

Instructions on the ROI form advise the Worker of the purposes of collecting the information, how to obtain a copy, correct or update their information.

The primary purposes of collecting, holding, using and disclosing information is to ensure that the Worker is suitably qualified to safely perform the task they are being sent to the Asset Owners site to perform and to effectively manage the complex logistics associated with a mobilisation event.

Each Worker completing a ROI must sign the form to acknowledge their consent to their personal information being collected and used for the purposes defined on the form. It is a compulsory condition of use set by Bright People Technologies that Asset Owners and their contracting companies retain a signed copy of the ROI form on their personnel files to verify the Worker's consent to the collection and use of their personal information.

ACCESS AND CORRECTION OF PERSONAL INFORMATION

Authorised Users and Worker's can, subject to the Australian Privacy Principles, request a copy of their personal information held on the ENABLE System by contacting us at: info@brighttechnologies.com.au. It is important to us that the personal information we hold is accurate, complete and up to date. If an Authorised User or Worker believes that this is not the case and would like their personal information updated or corrected, they may contact us at: info@brighttechnologies.com.au, (08) 9226 2828 or P.O. Box 1010 West Perth WA 6872.

For privacy and security purposes, we may ask that a request be put in writing along with specified information to verify the requestor's identity.

CONFIDENTIALITY

Information held on Authorised Users is available to the Asset Owner/s that requested the Authorised User's access to the ENABLE ERMS System.

Information held on Workers submitted to the ENABLE ERMS System is available to the Authorised User who submitted the data and other Authorised Users of the same company. The Worker's information is also available to the Asset Owner of the Site for which the Authorised User submitted the Worker's information.

Information held on Workers may be available to approved third party suppliers engaged by Bright People Technologies. Such parties are engaged for the purposes of providing software development and maintenance services; hardware and network security and support. Other than authorised use by Bright People Technologies staff, Authorised Users, Asset Owners and approved third parties as described above, information held on the ENABLE ERMS System is kept strictly confidential.



Security and Privacy Policy

HOW WE HANDLE EMAIL

We will preserve the content of any email we receive, if we believe that we have a legal requirement to do so. The content of email messages may be monitored and viewed by our employees and approved third parties for the purpose of responding to requests for assistance and quality of service.

SECURITY OF INFORMATION

All users of ENABLE ERMS have a unique user name and password. Users connect to the ENABLE ERMS application programs which interpret the requests for service, then connect to the databases for access to the underlying data.

Any connection to the database is secured across the Internet using SSL security encryption, certified by the InstantSSL Certificate Authority.

The ENABLE ERMS database and web interface is housed in a secure data centre with uninterruptible power supply and backup generator. The centre is air-conditioned with backup redundant air conditioning units and humidity monitoring and secured with swipe card access and 24 hour on site building security. The server has a 100 Mb connection to the Internet through a Firewall.

The ENABLE ERMS database and web interface is supported by dual server redundancy and are backed up daily in accordance with Bright's back up plan.

Bright regularly reviews developments in security and encryption technologies. Unfortunately, no data transmission over the Internet can be guaranteed as totally secure. Accordingly, although we strive to protect such information, we cannot ensure or warrant the security of any information transmitted to us or from our on-line systems or services and Authorised Users do so at their own risk. Once we receive a transmission from an Authorised User, we take reasonable steps to preserve the security of the information in our own systems.

All employees of Bright are required to enter into Confidentiality Agreements. The induction process for new employees of Bright includes training on the privacy obligation of both the employee and Bright.

ACCEPTANCE AND CHANGES TO SECURITY AND PRIVACY STATEMENT

Authorised Users acknowledge and accept that use of the ENABLE System indicates their acceptance of the ENABLE System "Terms and Conditions of Use" and this Security and Privacy Statement.

This is our current Security and Privacy Statement: Date of Publication 9 May 2012, Version 1.4.

We may at any time vary the Security and Privacy Statement by publishing the varied Security and Privacy Statement on the ENABLE ERMS System. Authorised Users accept that by doing this, Bright People Technologies has provided them with sufficient notice of the variation.

FURTHER INFORMATION

Further information about an individual's rights under the Privacy Act can be obtained from the Office of the Australian Information Commissioner Enquiry Line on 1300 363 992 .

Any further inquiries about our Security and Privacy Statement or inquiries or concerns about how any personal information is managed can be directed to us at: info@brighttechnologies.com.au (08) 9226 2828 or P.O. Box 1010 West Perth WA 6872.