PRIVACY POLICY

REFERENCE:	TBG v.07 | 10/2025
JURISDICTION:	Australia
OWNERSHIP:	Group Quality and Compliance
AUTHORISED BY:	Executive General Manager – Corporate Services
REVIEW:	10/2027

PURPOSE

The purpose of this policy is to ensure that all information collected, used, stored and disclosed by The BUSY Group Australia and its related bodies corporates (**TBG**, **BUSY**) is done so in accordance with provisions in the *Privacy Act 1988 (Cth),* the *Australian Privacy Principles* (APPs), freedom of information (FOI) and social security law, and relevant state-based privacy legislation. This policy also provides direction to TBG employees in relation to their obligations and expectations in relation to the handling of personal information and the protection of our customers' privacy.

Employees should refer to the Request For Information Procedure to provide internal guidance in relation to the process for handling requests for information received from customers directly or via external parties (under the *Freedom of Information Act* (FOI) or access provisions in the *Privacy Act 1988* (APP 12).

This Privacy Policy is publicly available on our websites and can be provided in alternative formats (such as hard copy) upon request by contacting The BUSY Group on privacy@thebusygroup.com.au (APP 1.5).

SCOPE

This policy applies to all current and former employees, directors, contractors and volunteers within **TBG Australia** and all related bodies corporate.

SAFEGUARDING COMMITMENT

As an organisation that prioritises the safeguarding of all vulnerable people, TBG is committed to providing a safe environment across all we do by actively adopting strategies that embed a culture of zero tolerance for abuse of any kind.

DEFINITIONS

a) ***Access*** means viewing**,** obtaining or retrieving personal information**.**

b) ***Anonymisation*** means removing all identifiable elements so individuals cannot be re-identified.

c) ***Confidentiality*** means limiting access to personal information, keeping it from those who do not have permission to see or hear it.

d) ***Consent*** is the free, voluntary and ongoing agreement to participate and must be clear, informed and specific.

e) ***De-identified/de-identification*** means that a person's identity is no longer apparent or cannot be reasonably ascertained from the information or data. *De-identified information* is information from which the identifiers about the person have been permanently removed, or where the identifiers have never been included.

f) ***Disclosure*** is the process of divulging information to a person outside TBG.

g) ***Eligible data breach*** arises when the following three criteria are satisfied:

1. there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds,
2. this is likely to result in serious harm to one or more individuals, and
3. the entity has not been able to prevent the likely risk of serious harm with remedial action

h) ***Government Related Identifier*** – has the meaning given to it in section 6(1) of the *Privacy Act*. An 'identifier' can consist of any number, letter or symbol, or a combination thereof, used to identify or verify an individual (with the exception of ABN's and names). When assigned by a government agency, a State or Territory authority, or a contracted service provider acting on their behalf (i.e. Medicare or Dept of Transport) it becomes a *government related identifier*.

i) ***Health information*** is any information or opinion about a person's mental or physical health or wellbeing. Health information includes any information relating to a person's access to health services.

j) ***Loss*** refers to the accidental or inadvertent loss or theft of physical devices, or paper records that contain personal information, in circumstances where it is likely to result in unauthorised access or disclosure.

k) ***Privacy*** is the right to control access to oneself and related information, including control of the type and purpose of information collected.

l) ***Permitted General Situation*** *has the meaning given to by section 16A of the Privacy Act*

m) ***Personal information*** directly or indirectly identifies a person. Personal information may include 'protected information' and 'sensitive information'.

n) ***Protected Information*** is defined in the *Social Security Act* (subsection 23(1)). Of relevance is paragraph (a) of the definition. It provides that 'protected information' means; *Information about a person that was*

obtained by an officer under the social security law; and is held or was held in the records of the department (DEWR) or Services Australia. Confidentiality provisions in the *Social Security (Administration) Act* prohibit any person from disclosing 'protected information' without authority from the government agency who owns the information (under a PIC).

o) ***Pseudonymisation*** refers to the replacing of identifiers with pseudonyms, while retaining the ability to re-identify under controlled conditions.

p) ***Reasonable steps*** *(as per APP 11.1 and APP 11.3)* has the meaning given to it by APP 1 *and* includes *'technical and organisational measures',* including protecting information through physical measures, software and hardware, whilst *organisational measures* include steps and processes that TBG has implemented, such as employee training on privacy and data protection. Further information can be found under 1. Commitment to Privacy.

q) ***Related body/ies Corporate*** – has the meaning given to in the *Privacy Act 1988* s.13B.

r) ***TBG***, ***BUSY***, ***employees, we, us, our*** refers to the current and former management, employees, volunteers, contractors and Board Directors of all the entities and programs of **The BUSY Group Australia.**

s) ***Use*** refers to the collection, handling, access, distribution, processing, analysis or application of information by staff where the information stays within the organisation. ***Unauthorised access*** occurs when personal information is accessed by someone who is not permitted to have access.

t) ***Unauthorised disclosure*** occurs when the entity makes personal information accessible or visible to others outside the entity, in a way that is not permitted by the *Privacy Act*.

u) ***Unsolicited personal information*** refers to personal information that has been collected by means outside of the definition of 'solicits' as given to it in s.6.(1) of the *Privacy Act 1988 (Cth)*. TBG will assess all *unsolicited personal information* received to determine whether it could have been collected under APP 3. If not, the information will be destroyed or de-identified as soon as practicable.

RESPONSIBILITIES

Employees

Employees of TBG are responsible for the appropriate handling of the personal information to which they have access, in line with this policy and regulatory and contractual obligations.

Post-Employment Privacy and Confidentiality Obligations

All employees, directors, contractors, and volunteers are required to maintain the confidentiality and privacy of personal and sensitive information obtained during the course of their engagement with TBG. These obligations continue after the termination of employment or engagement, regardless of the reason for departure.

Former employees must not disclose, use, or retain any personal information relating to clients, customers, staff, or other stakeholders unless expressly authorised or required by law. Under the *Privacy Act 1988* and the statutory tort for serious invasions of privacy (introduced in June 2025) individuals may be held personally liable for:

- Intentional or reckless misuse or disclosure of private information;
- Intrusion into private affairs without lawful justification;
- Any act that results in a serious invasion of privacy, where the affected individual had a reasonable expectation of privacy.

TBG and the departments we contract to maintain the right to take legal action, including seeking damages or injunctive relief, against any former employee who breaches these obligations.

Management

Management is responsible for:

- ensuring that the systems and processes referred to in this policy are in place to protect the privacy and confidentiality of our customers and stakeholders as outlined herein;
- ensuring employees have completed all privacy training required by TBG, our funding bodies or partners;
- ensuring employees are aware of their obligations in relation to this policy and under legislation,
- supervising employee's compliance to this policy and privacy legislation, and reporting and addressing any breaches that occur.

Privacy Officers

TBG Australia Privacy Officers include the Group Quality and Compliance Manager and a nominated member of the Information Technology Team. They will assist managers to ensure all employees are familiar with the Privacy Policy and administrative procedures for handling personal information, support management with complaints or privacy incidents, and conduct regular reviews of information management processes across the organisation to ensure they are robust and adapting to ongoing changes in the regulatory and operational environment.

The Privacy Officers can be contacted by:

Email: privacy@thebusygroup.com.au

Phone: 13 28 79

1. Commitment To Privacy

TBG are committed to respecting and protecting the privacy of our customers and stakeholders by ensuring individuals are informed about the personal information we collect and its purpose, asked for consent before collecting sensitive data or sharing information externally, granted access to their information upon request in accordance with relevant legislation, and made aware of their right to withhold or withdraw consent at any time, along with the implications of doing so.

As an APP entity, TBG will adhere to the APPs in its information management practices (the *collection*, *use*, *storage* and *disclosure* of personal information), which includes taking '*reasonable steps'* to protect personal information it holds from *misuse*, *interference* and *loss*, as well as *unauthorised access*, *modification* or *disclosure*, as outlined under APP 11.1.

'Reasonable steps' includes the implementation of practices, procedures and systems such as;

1. Procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification.
2. Security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails (in line with *International Standard ISO:27001*) (APP 11).
3. Procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries.
4. Procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity, in particular circumstances and where practicable (APP 2)
5. Governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and escalation of relevant information around notifiable breaches to TBG's governance body)
6. Regular staff training and information bulletins on how the APPs apply to TBG, and its practices, procedures and systems developed under APP 1.2
7. Appropriate supervision of employees regularly handling personal information, and reinforcement of practices, procedures and systems implemented in line with the APP 1.2
8. Mechanisms to ensure that agents and contractors in the service of or acting on behalf of TBG comply with the APPs.
9. A program of proactive review and audit of the adequacy and currency of TBG's Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

TBG commits to following departmental specific guidelines relating to privacy, to ensure that it meets its ethical, regulatory and contractual obligations in relation to protecting the privacy of customers referred to our services.

2. Collection of Personal Information

In collecting personal information, TBG will:

1. Only collect and store personal information that is reasonably necessary for, or directly related to the organisation's functions and activities
2. At the time of collecting personal information, provide individuals with a privacy notice (as per APP 5) outlining the purpose of collection, how the information will be used, and to whom it may be disclosed (APP 3). If sensitive information is being collected the notice will also confirm the *consent* of the individual (APP 3.3(a), unless an exception applies. Notices will be provided in writing or verbally, depending on the context.
3. Collect personal information from the individual directly (APP 3.6), unless the individual consents to the collection of their information from a third party, or one of the exceptions apply.
4. Upon request, individuals will be provided with information in relation to how their personal information is stored, how long it will be retained for and how they can gain access to it for correction or release.
5. *Unsolicited* information received will be handled in accordance with APP 4, which may involve being destroyed or de-identified, would it not have been collected with consent from the individual.
6. Use reasonable means to ensure information being provided by other agencies or external parties conforms to the privacy principles.
7. Publish this Privacy Policy and a privacy collection notice in relation to information collected via the organisation's websites.

2.1 Anonymity and Pseudonymity

Where lawful and practicable, individuals may choose to interact with us anonymously or by using a pseudonym (such as a preferred name), in line with APP 2. However, due to the nature of the programs and services TBG administer, it may often be impracticable to provide services without verifying identity. In circumstances where identification is required by law or our contractual obligations, or necessary to deliver services effectively (e.g. job placements, eligibility for funding), we will request and collect personal information. We will inform individuals when identification is necessary and ensure that any personal information collected is handled in accordance with this Privacy Policy and the APP's.

3. Use and Disclosure of Personal Information

TBG will ensure that:

1. Personal information held by the organisation will only be used or disclosed for the *primary* purpose for which it was collected unless the individual has consented to a secondary purpose (APP 5), or in the following situations:
   a) the information is directly related to the primary purpose
   b) the use or disclosure of the information is required by law or court / tribunal order,
   c) a *'permitted general situation'* exists, for example;
      i. TBG reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety
      ii. TBG has reason to suspect that unlawful activity, or misconduct of serious nature that relates to the entity's functions or activities has been, is being, or may be in engaged in.
      iii. when believed necessary for enforcement related activities on behalf of an enforcement body (e.g. for a criminal investigation by the police).
2. *Protected information* of customers contained in any government or third-party system is only accessed by authorised employees in relation to the work-related service or primary purpose (i.e. for a business need, not for personal interest or gain). Employees found to be accessing customer records without a business need may face disciplinary action, termination of employment and possible criminal charges.
3. Information recorded or conversations regarding individuals remain objective and have regard to the individual's privacy and dignity.
4. Individuals will be provided with the opportunity to request a private space (i.e. interview room) when they are discussing matters of a personal or sensitive nature.
5. Personal information is only used for direct marketing activities where the individual has full knowledge of the type of information used, how the information will be used and with specific consent from the individual. Individuals may 'opt-out' of receiving direct marketing communications at any time by contacting TBG or using the opt-out mechanism provided in the communication.
6. If data is released for data projects/research purposes to other bodies corporate of TBG or to a third party (i.e. a university or Government Department), it will be *de-identified* as required, to preserve the privacy of individuals.
7. *Cross-border disclosures of personal information (APP 8)* - Where TBG is subject to strict contractual obligations or system-based restrictions that prevent overseas access, personal information will not be disclosed to parties outside Australia. If cross-border disclosure is required,

TBG will take reasonable steps in line with APP 8 to;

a) Notify the customer (APP 5) that their personal information may be disclosed overseas, including which countries (if practicable) and the purpose of the disclosure.

b) Ensure the overseas recipient complies with the APP's in relation to personal information. This includes ensuring that the recipient is subject to substantially similar privacy laws and that individuals can enforce those protections and/or entering into contractual arrangements that safeguard personal information by requiring compliance with the APP's.

There are exceptions to APP 8, such as where the individual has consented after being expressly informed, or disclosure is necessary to prevent a serious threat to life, health or safety or for suspected unlawful activity or misconduct.

If a customer has concerns about the transfer of their information overseas, they may contact us using the details provided in this policy.

3.1 Adoption, Use and Disclosure of Government Identifiers

APP 9 restricts the adoption, use and disclosure of government related identifiers. Examples include Job Seeker Identification number (JSID), Tax File Number (TFN), Customer Reference Number (CRN), Medicare card numbers, Passport and driver licence number.

Generally, TBG must not adopt a government related identifier as its own, or use or disclose a government related identifier, except where it is necessary to provide services under contracts with the department.

This means government related identifiers should not be disclosed to or included in communications with third parties, except when necessary in communications with the department or other contracted service providers (i.e. employment services providers).

TFNs of individuals (not corporate entities) are subject to additional requirements under the *TFN Rule 2015* and must be **redacted** on all documentation before being saved to any system or CRM, including the departments systems.

3.2 Withdrawal of Consent to Release Personal Information

TBG will ensure that;

1. Individuals are informed of their right to withdraw their consent to obtain and release information at any time
2. The process for withdrawal of consent is easy and accessible (i.e. verbal or in writing to an authorised TBG employee of the program they are engaged with)
3. The individual is informed of the possible consequences of withdrawing their consent (i.e., their

mutual obligations will not be affected but there may be limitations to the provision of services)

4. Once an individual has withdrawn consent, the organisation cannot rely on the individual's past consent for any future use or disclosure of personal information.
5. the withdrawal of consent will be recorded on the individual's record.

3.3 Use of Artificial Intelligence (AI)

TBG may use artificial intelligence (AI) technologies to enhance our services and support internal operations such as data analysis, customer support, and quality assurance. If AI tools are used to process personal information, it is done in accordance with all applicable privacy laws and our privacy and data protection policies, including the *TBG ISMS Artificial Intelligence (AI) Policy*. We ensure that any AI systems used are subject to appropriate oversight, and we take reasonable steps to safeguard customer privacy and data security. We provide mechanisms for customers to query or advise us of concerns around the use of AI in relation to their personal information.

4. Storage & Security of Personal Information

TBG will ensure:

1. Electronic records are stored in line with applicable information security standards (i.e. ISO:27001, RFFR and DISP) and are protected by password security - employees are expected to ensure their computers remain locked whilst unattended and portable devices remain secure, both onsite and offsite. Hard copy participant files will be stored in locked cabinets to prevent unauthorised access.
2. When hard copy customer information is being utilised or electronic customer records are open, care will be taken to ensure that personal information is not visible to or accessible by anyone not authorised to access the information.
3. *Reasonable steps* are taken to protect all personal information from misuse and loss and from unauthorised access, modification or disclosure (APP 11).
4. In the event of unauthorised access to, unauthorised disclosure of, or loss of personal information, TBG will respond to the incident in line with the requirements under the APPs and the Office of Information Commissioner (OAIC) Notifiable Data Breaches (NDB) Scheme. See section 7. Privacy Incidents and Data Breaches.

4.1 De-identification Practices

To support service improvement and research, TBG may share data within the related subsidiary entities of the corporate group (non-sensitive personal information) or with a third party (i.e. a university or the Department). In doing so, and in accordance with APP 11, TBG will preserve individuals' privacy by using

de-identification techniques such as *anonymisation* or *pseudonymisation*. These techniques are used to ensure that data used for analysis, reporting or research purposes does not constitute personal information. By removing or altering personal identifiers, TBG ensures that the information cannot reasonably be used to identify individuals, in accordance with applicable privacy laws and ethical standards. TBG will comply with all APPs in the handling of this data.

4.2 Retention and Disposal of Personal Information

1. Personal information is destroyed or permanently de-identified when it is no longer needed and/or after legal or contractual requirements for retaining information have expired.
2. The retention and destruction of personal information will be actioned in accordance with relevant TBG ISMS and QMS policies, and regulatory and contractual obligations.
3. Personal information contained in hard-copy records will be disposed of via secure shredding disposal containers. At least one appropriate disposal unit is to be kept in each physical location.

5. Access and Correction of Personal Information

In line with APP 12 and 13 TBG will:

1. Take *reasonable steps* to ensure personal information collected, stored or disclosed is accurate, complete and up to date, having regard to the use and disclosure (APP 10).
2. Upon request;
   a) Provide access for an individual to review information or correct information about themselves, unless an exception applies (APP 12 and 13)
   b) In line with the access provisions in the *Privacy Act* and *Freedom of Information Act*, provide access to individuals to the information that TBG holds about them. TBG employees can refer to the internal Request For Information Procedure for further details on how to process a request for access to information from a customer.
   c) Ensure corrections are made to the personal information held by the TBG; or notify another entity where the personal information corrected has been previously disclosed to that entity, free of charge and without recourse. Corrections can be made to information by updating the record or document and adding a notation or file note.
3. Where a request to access or correct information is refused, advise the individual in writing of the reasons for the refusal and provide information on how they can make a complaint about this decision.

6. Employee records

1. Due to the '*employee records exemption'* within section 7B (3) the *Privacy Act 1988*, it generally does not cover personal information held by private organisations about their employees, specifically when the 'information relates directly to a current or former employment relationship' (i.e. personal & emergency contact details, employment terms and conditions, training and performance information and taxation & banking details). This exemption only begins once the individual is considered an *employee*, so does not apply to information regarding job applicants, candidates, or independent contractors.
2. The exemption does not apply to TFN information within an employee record.
3. TBG will only use information collected from employees for purposes directly related to their employment. If TBG wishes to use the information for a purpose that could be considered outside the employment relationship (i.e. images of social events used for marketing purposes on company websites) the employee will be notified and given the opportunity to provide or withdraw their consent, as required by law.
4. If TBG experiences a data breach involving employee information captured during and directly related to the course of their employment, the notification and handling requirements under the *Privacy Act* may still apply.
5. TBG will abide by provisions in any state-based legislation covering employee records (i.e., whereby employees can request access to their personal information and seek correction of inaccurate or outdated information).
6. If personal information of employees (considered to be outside of the employment relationship) is captured in the course of tracking and monitoring information transmitted or received by TBG's monitoring systems, it will be treated as *unsolicited personal information* in accordance with the APPs.
7. The storage of personal information and documentation by employees on TBG systems or resources (i.e., company issued laptops and mobile phones) is discouraged and is done at their own risk. Responsibility will not be taken by TBG for unintended disclosure, unauthorised access, or loss in relation to that unsolicited personal information.

7. Privacy Incidents and Data Breaches

A privacy incident or data breach occurs when personal information held by an organisation is subjected to **loss**, **unauthorised access** or **unauthorised disclosure**.

In the event of an information security or privacy incident TBG employees should refer to the internal

Information and Privacy Incident Reporting Process which outlines in detail;

1. Immediate actions that can be taken to contain the breach and mitigate the risk of harm to affected individuals
2. Required process to report the incident to Management and Group Compliance, who will notify the Department associated with the relevant program, subcontracting partners (i.e. CoAct), affected individuals and the Information Commissioner, as required.

An assessment will carried out by Management to determine if the data breach is considered an '*eligible data breach*' (refer to definitions) under the Notifiable Data Breach Scheme (NDBS). The NDBS scheme applies to government agencies and private sector and not-for-profit organisations, such as TBG, who are currently subject to the Australian Privacy Principles, specifically APP 11 (*APP Entities*).

The assessment will be performed promptly after Management become 'aware' of the incident, as the risk of serious harm to individuals often increases over time, and all *reasonable steps* must be taken to complete the assessment within a maximum of 30 calendar days (as per s26 WH (2) of the *Privacy Act 1988*).

If the incident is deemed to be an '*eligible data breach'*, TBG's response will be in accordance with the requirements of NDBS and the *TBG ISMS Cyber Security Incident Management and Data Breach Response Policy.* This may include notification to affected individuals or the Office of Australian Information Commissioner (OAIC).

Notification to affected individuals is only required if the data breach is assessed as being an '*eligible data breach*'. If the incident is not deemed to be an *eligible data breach* TBG may decide to voluntarily notify affected individuals. This determination will be made by the Program Management in consultation with Group Compliance and IT as required.

Actions arising from these incidents will be reviewed as part of the continuous improvement to strengthen BUSY's processes.

9. Privacy Inquiries or Complaints

If a customer wishes to make an inquiry or complaint about the handling of their personal information, they may contact TBG via;

1. Email to the Privacy Officers at privacy@thebusygroup.com.au
2. Phone 13 28 79
3. The Feedback Form on the website

Please refer to our Grievance Policy and Feedback & Complaints Procedure for detail on how we investigate and manage complaints.

If the customer is not satisfied with how TBG has dealt with their privacy inquiry or complaint, they may apply to the Australian Information Commissioner for an external review.

10. Review

This policy is subject to review **every 2 years** or when there is deemed to be material changes to privacy legislation or contractual obligations that require incorporation.

TBG will ensure compliance against the legislation outlined within this policy is maintained, via regular audits and reviews, to assess the effectiveness of privacy practices and identify areas for improvement (APP 1).

11. Policy Context and Resources

This policy relates to the following legislative requirements, standards and internal TBG documents:

Legislation

- Australian Privacy Principles (APP's)
- Privacy Act 1988 (Cth)
- Social Security Act 1991 (Cth)
- Social Security (Administration) Act 1999 (Cth)
- Social Security Guide (confidentiality provisions/protected information)
- Freedom of Information Act 1982 (Cth)
- Australian State and Territory Privacy Legislation

Related Forms & Documents

- Privacy Notification, Collection and Consent forms
- Authority to Gain and Release Information forms
- Publicity Consent Forms
- Photographic and Media Release Permission forms
- Workforce Australia *Part A Guidelines* and associated *Privacy Guideline*
- Request for Information Procedure
- TBG Information Security Management System (ISMS)
- TBG ISMS Artificial Intelligence (AI) Policy
- TBG Information Security Policy
- TBG ISMS Backup and Restore Policy
- TBG ISMS Clear Desk and Clear Screen Policy
- TBG Cyber Security Incident Management and Data Breach Response Policy
- TBG Security Clauses for Third Party Suppliers
- Feedback & Complaints Procedure
- Grievance Policy
- Safeguarding Risk Management Framework
- Information and Privacy Incident Reporting Process

12. Version Control

Version	Date	Change Summary	Author/Reviewer	Approved by:
7	October 2025	• Added clauses to cover: ○ Post employment obligations ○ Government related identifiers ○ Employee records exemption ○ Artificial Intelligence (AI) ○ Withdrawal of consent ○ Incorporation of first tranche of reforms from *Privacy and Other Legislation Amendment Act (Cth)* Dec 2024 – inclusion of clause for 'reasonable organisational measures' & civil tort for serious privacy invasions which extends post-employment. • Included references to the relevant APPs. • Separation of the Request for Information Procedure (internal SOP document) from this public facing policy. • Approver changed from GCEO to EGM CS.	Group Quality and Compliance Manager	Executive General Manager - Corporate Services
6	October 2023	Replaced Child Safety Commitment with revised Group Safeguarding Commitment Inserted - section in relation to personal information of employees, additional Management responsibilities, definitions in relation to Incidents, and amended references to Access.	Group Compliance Manager	Group Chief Executive Officer
5	June 2023	Ownership from People & Culture Manager to Group Compliance Manager Insert sections for PIC's Insert section for 'withdrawal of consent' Inserted definition for 'protected information' Inserted definition for 'delegated person' Amalgamation of the 'Request for Information Procedure' into this Privacy Policy	Group Compliance Manager	Group Chief Executive Officer
4	September 2022	Review, minor updates	People & Culture Manager	Group Chief Operating Officer
3	September 2020	Change from ON-Q to BUSY Ability	Group Compliance Manager	Chief Operating Officer – The BUSY Group
2	August 2020	Child safety commitment included and change of Privacy officer	HR Manager	Managing Director – The BUSY Group