Privacy Policy

POLICY:

Vivid is committed respecting the privacy of the personal information it holds about individuals and that it is handled appropriately and lawfully.

SCOPE:

This policy, and the following procedures, apply to all Vivid employees in their dealings with personal information about clients, customers, contractors, consultants, students, other employees and job applicants.

DEFINITIONS:

Personal Information - information which identifies an individual or from which an individual's identity can be reasonably ascertained and includes Sensitive Information. Names, addresses and home telephone numbers are examples of Personal Information.

Sensitive Information - includes information or an opinion about an individual's racial or ethnic origin, political opinions, philosophical or religious beliefs or affiliations, membership of a political, trade or professional association or trade union, sexual preferences or practices, criminal record or Health Information.

Health Information - information or an opinion about individual's physical, mental or psychological health, disability, health services and donation of body parts, including genetic information.

PROCEDURES:

1. General

1.1 Employees must collect and handle Personal Information in accordance with this Policy and take reasonable steps to protect any Personal Information in their care from misuse, loss, unauthorised access, modification and disclosure. This can include measures such as:

1.1.1 storing Personal Information in locked filing cabinets;

1.1.2 having a clean desk policy;

1.1.3 not allowing others to use an employee's' computer passwords; and

1.1.4 not gossiping about personal details concerning others.

This list is by no means exhaustive and the security measures taken should be those that are reasonable in the circumstances.

1.2 If an employee has any concerns about the way in which Personal Information is being handled, or believes there has been an interference with the privacy of any individual, they should contact the Privacy Officer (jodie.bell@wearevivid.org.au).

2. Collection of Personal Information

2.1 Vivid will only collect Personal Information that is necessary for its business functions and activities, including complying with legal or regulatory obligations. Vivid will collect Personal Information by lawful and fair means and not in an unreasonably intrusive way.

2.2 When Vivid collects any Personal Information, Vivid will take reasonable steps to provide the person (whose Personal Information is being collected) information about:

2.2.1 the identity of Vivid and how to contact it;

2.2.2 why Vivid is collecting the Personal Information;

2.2.3 the intended recipients of the information, including the types of organisations (if any) to which Vivid may disclose the Personal Information (e.g. payroll processing services);

2.2.4 their right to request access to their Personal Information;

2.2.5 any law that requires the particular information to be collected; and

2.2.6 the main consequences for failure to provide that information.

2.3 Where reasonable and appropriate, Vivid will collect Personal Information directly from the individual, however there are certain situations in which Personal Information about an individual may be collected from someone else. In either case, Vivid will take reasonable steps to notify the individual of the matters listed above.

2.4 In certain circumstances Vivid may collect Sensitive Information or Health Information. Vivid will only collect this information with the consent of the person whose information is being collected, or otherwise in accordance with the law.

3. Use and Disclosure of Personal Information

3.1 Personal Information will generally be used or disclosed for purposes related to the main purpose(s) for which it was collected.

3.2 Where Vivid needs to use or disclose Personal Information for purposes other than these purposes, Vivid will obtain consent where appropriate and necessary. Exceptions to this include where:

3.2.1 the use or disclosure is required to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or to public health and safety;

3.2.2 Vivid suspects fraud or unlawful activity;

3.2.3 the use or disclosure is necessary to assist a law enforcement agency in its law enforcement functions; or

3.2.4 the use or disclosure is required or authorised by or under law.

4. Quality and Accuracy of Personal Information

4.1 Vivid will take reasonable steps to ensure that any Personal Information Vivid uses or discloses is complete, accurate and up-to-date.

4.2 If an employee becomes aware that any Personal Information Vivid holds is not accurate, they must notify the Privacy Officer (jodie.bell@wearevivid.org.au) promptly.

5. Retention and Destruction of Personal Information

5.1 Vivid will only keep Personal Information on file for as long as it is necessary to fulfil business needs or legal requirements.

5.2 When Vivid no longer requires the Personal Information, Vivid will destroy or dispose of it in a secure manner.

6. Access to and Correction of Personal Information

6.1 Individuals generally have a right to request access to any Personal Information which Vivid holds about them. There are a number of exceptions to this principle including:

6.1.1 where providing access would pose a serious and imminent threat to the life or health of any individual;

6.1.2 where providing access would have an unreasonable impact upon the privacy of other individuals (this may be relevant where information about other individuals is included on a file);

6.1.3 the request for access is frivolous or vexatious;

6.1.4 the information relates to existing or anticipated legal proceedings where the information would not otherwise be discoverable;

6.1.5 providing access would be unlawful;

6.1.6 denying access is required by law;

6.1.7 providing access would prejudice an investigation of possible unlawful activity; and

6.1.8 providing access would prejudice law enforcement.

6.2 Requests for access should be forwarded to the Privacy Officer (jodie.bell@wearevivid.org.au).

6.3 If access is to be denied on any of the grounds listed above, the denial of access must be authorised by the Privacy Officer (jodie.bell@wearevivid.org.au).

6.4 If an individual's request for access to the Personal Information is denied, Vivid will provide the person with reasons why this is the case.

7. Notifiable Data Breach Scheme (NDBS)

7.1 It is the responsibility of all Employees to minimise the risk of loss or unlawful access (data breach) of personal information by implementing the security measures outlined in this Policy and in the Information Technology Policy.

7.2 A data breach maybe an "Eligible Data Breach" under the NDBS where there has been:

7.2.1 Unauthorised access (such as by a hacker accessing client information through Vivid's website) to personal information; or

7.2.2 Unauthorised disclosure (such as an Employee inadvertently, or deliberately, handing over a client's information to an external person) of personal information; or

7.2.3 A loss (such as an Employee losing their smartphone in a public place) of personal information.

7.3 It is the responsibility of all Employees to immediately report any data breach, or suspicion of a data breach, to the Privacy Officer.

8. Correction

8.1 Individuals may request to correct their Personal Information. Vivid will make such correction or, if unsure whether such correction is appropriate, refer to the Privacy Officer (jodie.bell@wearevivid.org.au) for guidance.

8.2 If Vivid refuses to alter the information, Vivid will provide the individual with reasons why this is the case and include a statement about the disputed facts on their file.

8.3 Vivid will take reasonable steps to protect Personal Information and to safeguard Personal Information from misuse, loss and unauthorised access, modification and disclosure.

9. Complaints Procedure

9.1 If an individual complains about their Personal Information being inappropriately handled, then that complaint should be immediately referred to the Privacy Officer (jodie.bell@wearevivid.org.au).

9.2 Complaints will be handled impartially and as promptly as possible in the circumstances. Only those people who are involved in the investigation of the complaint will have access to Personal Information in relation to the complaint.

10. Inability to Give Consent

10.1 In some cases, the people Vivid supports may not be able to give consent because they are unable to do so. In these cases, the individual will have selected an advocate (usually a family member) to make decisions and sign consent forms, on their behalf. This consent will be kept on the client's SupportAbility file.

11. Photographic and Video Material

11.1 Vivid will only use images of clients if they have agreed for this to happen by signing a release on their Personal Information & Signed Consent form.

12. Failure to comply

Failure to comply with this policy may result in disciplinary action in accordance with the Disciplinary Policy. This may include informal counselling, warnings or termination of employment.

13. Related Policies and Documents

Other policies and documents which are relevant to the Privacy Policy include:

13.1 Records Management Policy;

13.2 Notifiable Data Breaches Scheme

Version Control

V1.0 - 27/9/2017	V1.1 - 13/11/2019	V1.2 – 26/10/2020			