Confidentiality and Data Protection Policy

Contents

1. Aims and Objectives

1.1. This policy is set out to identify how Segon-Marill International Movers PLC executes its duty to keep clients and employees personal information safe and confidential whilst at the same time, not compromising its ability to share information where it is needed.

1.2. The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within the organization including volunteers and have access to clients and employees personal information.

1.3. Segon-Marill is committed to maintaining the confidentiality of clients and employees personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose, or passed to a third party, without their consent except in special circumstances e.g. to prevent harm to an individual.

1.4. Segon-Marill will ensure that personal information is obtained, used and disclosed in accordance with the Company's Code of Business Conduct.

1.5. Segon-Marill will also have full regard for current and future legal requirements which impinge on the confidentiality of:

1.5.1. Client's personal information in general, and

1.5.2.Specific categories of employees personal information

2. Principles

Client's personal information held in both computerized and manually filed records will:-

2.1. Be obtained and processed fairly,

2.2. Be used only for the specified purposes for which it was obtained and not in any manner incompatible with those purposes,

2.3. Be adequate, relevant and not excessive for those purposes,

2.4. Be kept accurate and where necessary up to date,

2.5. Not be kept longer than is necessary for those purposes,

2.6. Be protected from unauthorized access, unlawful processing, accidental loss, destruction or damage,

Not be transferred to a country, which does not ensure adequate protection for the rights of individuals in relation to the processing of personal information. In order to implement and properly maintain a robust information security function, Segon-Marill recognizes the importance of:

2.7. Understanding Segon-Marill's information security requirements and the need to establish policy and objectives for information security;

2.8. Implementing and operating controls to manage Segon-Marill's information security risks in the context of overall business risks;

2.9. Ensuring all users of Segon-Marill's information assets are aware of their responsibilities in protecting those assets;

2.10. Monitoring and reviewing the performance and effectiveness of information security policies and controls; and

2.11. Continual improvement based on assessment, measurement, and changes that affect risk.

3. Definitions

3.1. **'Confidentiality'** applies to information whether received through formal channels (e.g. in a formal report), informally, or discovered by accident. It applies to organizational business, employees and potential employees, volunteers, learners, clients, individuals, or organizations that come into contact with the organization i.e. external contractors/partners.

3.2. Information which can be classified as 'Confidential', can broadly be grouped into the following areas:-

3.2.1. **Information of a specific and personal nature about learner / clients, employees or volunteers**

If this type of information is used inappropriately, it can cause individuals to face discrimination, harassment or harmful actions and inappropriate decisions by others.

3.2.2.**Sensitive organizational information**

This may be used to damage the organization and other organizations, as well as individuals, staff or volunteers. It may be prejudicial to the business of the organization or used to threaten the security of its property and systems.

3.3. **Breaches in confidentiality** happen when sensitive information is given to people who are not authorized to access it.

3.4. **Information security** is the preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, and reliability can also be involved, agreed or followed. They can also happen when information is passed between sections, or organizations, or when information is being stored insecurely.

4. Informed Consent

4.1. Where it is proposed, in exceptional circumstances, that information about an individual should be shared with another agency or person, the consent of the individual, or the person who provided the information, should normally be sought.

4.2. This should be done in such a way that those persons know exactly what information will be passed on, to whom and for what purpose.

4.3. Information, which is confidential and restricted, will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.

4.4. Wherever possible informed consent should be recorded in writing as a form of contract which gives the agreed terms and conditions of passing on and storing this information.

4.5. Informed consent should be sought every time there is a need for confidential information to be passed on to an unauthorized person.

4.6. Confidential information will not be discussed on the telephone unless the identity of the caller is established, this will be checked when necessary, e.g. with call-backs and/or security checks prior to the release of any information.

4.7. Refusal to give consent should be respected wherever possible.

5. Employee Responsibilities

5.1. In normal circumstances, staff may only disclose personal information outside the organization if one or more of the following applies:

5.1.1. The disclosure is routinely necessary for the purpose for which the information is held and the individuals about whom the data is held have been made aware of, or could reasonably expect, such a disclosure to be made;

5.1.2. The receiving staff member 'needs to know' the information in order to carry out their duties;

5.1.4. The person about whom the information is held has given valid consent to the disclosure;

5.2. Where it is not possible to obtain valid consent, information may exceptionally be passed on when there is a legal basis for overriding the usual non-disclosure.

5.2.1. The disclosure is required under direction of a Court Order, or in the course of law enforcement,

5.2.2. The disclosure is provided for agreed inter-agency procedures which have a legal basis for their operation,

5.2.3. Where this is an overriding public interest in disclosing the information such as evidence of a risk of serious harm to the individual or in order to prevent or detect a serious crime.

5.3. When passing information to others, staff should:

5.3.1. Check that the source of the request is bona fide;

5.3.2. Ensure that the recipients understand and accept their obligation to respect the confidentiality of the information;

5.3.3. Only send the information necessary for the purpose of the disclosure;

5.3.4. Record exactly what has been passed on, to whom, when and why.

5.4. When receiving information from others, staff should:

5.4.1. Ensure that any information received in confidence should be marked as such to ensure it is not inadvertently disclosed to third parties;

5.4.2. Ensure that only information necessary for the purpose of the information being shared should be requested.

5.4.3. Ensure that information requests include a confidentiality statement similar to "Information will be treated with utmost confidence and will not be divulged to anyone outside the organization except when stated at collection or agreed at a later date." All confidential information shall be treated in line with Segon-Marill's Confidentiality & Data Protection policy. A copy can be requested from the Human Resource and Administration Section.

5.5. No reference to the company, its customers, suppliers or the work it undertakes must be made verbally or in any correspondence outside the company, in particular through social networking methods. Any information or reference to Segon-Marill passed through social networking must be approved in advance by the General Manager.

5.6. Before sharing sensitive commercial information with suppliers or customers a signed non-disclosure agreement (NDA) must be in place to ensure confidentiality is maintained.

All staff employment job descriptions and volunteer role descriptions must contain a statement enforcing the duty to respect the confidentiality of information. The employee handbook must include this obligation which then forms part of the employee's contract / volunteer's agreement.

5.7. Staff, students, staff of other agencies, temporary staff and volunteers will be asked to sign declarations of confidentiality on commencing employment with Segon-Marill either as part of their staff contract or as a separate statement.

5.8. All employees and volunteers are responsible for:

5.8.1. Checking that any personal data that they provide to Segon-Marill is accurate and up to date.

5.8.2. Informing Segon-Marill of any changes to information which they have provided, e.g. changes of address.

5.9. Sensitive information is only to be requested on a 'need to know' basis. This means only when the information is necessary to provide a service or to manage the delivery of a service effectively, and then only in the best interest of service users or staff.

6. Compliance

6.1. Segon-Marill will ensure that staff, volunteers and trustees receive adequate training and guidance on their duties and responsibilities in relation to the handling, disclosure and storage of personal information and information assets and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse.

6.2. Department Managers must ensure that staff and volunteers are made aware of the limits of their responsibilities, and where they may seek advice, should they have an information request which falls outside their responsibilities.

6.3. In accordance with the organization's disciplinary procedures, disciplinary action will be taken against any member of staff who fails to carry out the duties and responsibilities set out in this Policy or the procedures that follow from it.

6.4. Where contractors and employment agencies are used, the contracts between Segon-Marill and these third parties will contain clauses to ensure that contract staff are bound by the same code of confidentiality as employed staff.

6.5. Procedures will be implemented to ensure an employee's, contractors or third party's exit from Segon-Marill is managed and the return of all equipment and removal of all access rights are completed.

6.6. Any breach of this policy will be taken seriously and may result in formal action. Any employee who considers that the policy has not been followed in respect of personal data about themselves should raise the matter with their line manager or the Senior Human Resource and Administration Expert in the first instance.

7. Segon-Marill's Designated Data Controller

Segon-Marill is responsible for ensuring compliance with the implementation of this policy on behalf of the General Manager. The Information System Support Expert is the data creator and keeper and any questions or concerns about the interpretation or operation of this policy should be taken up in the first instance with the Senior Human Resource and Administration Expert.

8. Data Security

8.1. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

8.1.1. Any personal data which they hold is kept securely, either electronically or in lockable cabinets

8.1.2. Personal information is not disclosed either orally, in writing or otherwise to any unauthorized third party.

8.2. Documents containing individual data must not be left visible where it can be read by anyone inappropriately. This includes telephone messages, computer prints, letters and other documents.

8.3. Desks must be cleared each evening and electronic documents closed down when leaving a desk. Office layout should take the responsibility for personal data into consideration.

8.4. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords.

8.6. All hardware containing data must be housed in a secure environment.

8.7. Personal data must not be stored on the hard disc of a laptop or flash drive unless it has been encrypted.

8.8. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner including sufficient firewall.

8.9. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with Segon-Marill's policies.

8.10. The physical and environmental security will prevent unauthorized physical access, damage, theft, compromise, and interference with Segon-Marill's information and facilities. Locations housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls. Secure areas like the server room and the likes is protected by appropriate security entry controls to ensure that only authorized personnel are allowed access

9. Rights to Access Information

9.1. Data is classified into different categories according to the sensitivity and usage.

9.2. In accordance with individuals' rights of access under this policy, Segon-Marill will, on request, inform an individual whether or not information is kept about them and, if so, will provide a copy of that information. Any person who wishes to exercise this right should make the request in writing to the Information System Support Expert using the standard form. **(See Appendix I)**

10. Publication of Segon-Marill Information / Social Media or Website

10.1. Client feedback or testimonial can be publicized in our website with the written permission of same.

10.2. Under no condition should a staff publish or discuss information about Segon-Marill through personal social media whether or not they consider the information to be confidential. Exceptions would need approval by the General Manager.

11. Collection and Retention of Data

11.1. Any personal data collected that is not in the public domain should have the permission of the person relating to the information. Any business sensitive data should be agreed by a non-discloser agreement. In all cases the purpose for holding such data should be clear. Data with no clear purpose should not be collected or retained

11.2. Segon-Marill will keep some forms of information for longer than others depending on a number of factors e.g. for Marketing or data analysis purpose. All staff are responsible for ensuring that information is not kept for longer than necessary.

11.3. Disposal of information that are no longer required must be with regards to confidentiality, shredding paper documents and destroying other data in an appropriate manner.

11.4. The contents of each filing cabinet and each archive box of the clients and employees data are recorded on the filing cabinet and archive box lists with the File and Data Record and Human Resource and Administration Section.

12. Information Security Audit and Incident Management

12.1. Auditing of the various processes around data management is built into the standard audit cycle

to ensure compliance with this policy.

12.2. Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures is established and communicated to all employees. Responsibilities and procedures will be established to handle information security incidents once they have been reported.

Appendix 1

SUBJECT ACCESS INFORMATION REQUEST FORM

Under the Data Protection policy, you are entitled to request access to client's personal information held by Segon-Marill. Completing this form will help to get the information you require quickly and efficiently.

State the reason why data is needed

Declaration

Please read the following declaration carefully, then sign and date it. Please note that any attempt to mislead may result in prosecution.

I,_____(name) certify that the information provided on the information request form is true. I understand that it is necessary for Segon-Marill to confirm my/the data subject's identity and that it may be necessary for Segon-Marill to request more details from me in order to be able to locate the correct information.

Print Name: _____

Signature: _____ Date: _____

Checked By:

Date received: _____ Date responded: _____

NOTES:

_____

_____