DONEGAL TRAVELLERS PROJECT DATA PROTECTION POLICY – GUIDELINES

CONTENTS

INTRODUCTION

Under the Data Protection Acts, 1988 and 2003, Donegal Travellers Project as data controllers, have a legal responsibility to:-

– obtain and process personal data fairly;

– keep it only for one or more specified and explicit lawful purposes;

– process it only in ways compatible with the purposes for which it was given initially;

– keep personal data safe and secure;

– keep data accurate, complete and up-to-date;

– ensure that it is adequate, relevant and not excessive;

– retain it no longer than is necessary for the specified purpose or purposes; and,

– provide a copy of his/her personal data to any individual, on request.

The purpose of this policy is to assist Donegal Travellers Project in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help Donegal Travellers Project to meet their legal responsibilities as set out above. This policy has been created to reflect the specific requirements of Donegal Travellers Project.

SCOPE

This document provides guidelines on how personal data is to be stored, handled and protected under the following headings:-

a. General Procedures;
b. Paper Records;
c. Email and Personal Productivity Software;
d. Electronic Remote Access;
e. Laptops/Notebooks;
f. Mobile Storage Devices;
g. Data Transfers;
h. Inappropriate Access/Audit Trail Monitoring;
i. Breach Management.

EMPLOYEES

The information contained in this document is intended for general distribution to all employees of Donegal Travellers Project. However, it is especially important that the Project Manager and senior team leaders are aware of the contents of the document as the responsibility rests with them to ensure that the guidelines contained in it are followed. The guidelines should also be brought to the attention of all staff whose work involves the handling of personal data.

GENERAL PROCEDURES

This document sets out guidelines in a number of specific areas where particular attention should be paid in order to help protect the confidentiality of personal data held in Donegal Travellers Project. There are, however, a number of general procedures which Donegal Travellers Project should follow:-

1. The first stage in establishing policies and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be should that data be lost or stolen. The Donegal Travellers Project have conducted an audit identifying the types of personal data held within the organisation, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data is included in the Donegal risk register. Donegal Travellers Project can then establish whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document.

2. The financial/administration office is the location within the Port House Building where all personal data is stored and access is restricted only to those staff members that have permission to be there. There is a sheet/log at the front of vulnerable persons data file which record when, where and by whom the files was accessed. These access records and procedures are reviewed by management regularly.

3. Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified.

4. Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. If possible, password length should be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Donegal Travellers Project must also ensure that passwords are changed on a regular basis.

5. Donegal Travellers Project has procedures in place to properly evaluate requests from other organisations for access to personal data in its possession. These procedures assist Donegal Travellers Project in assessing whether the release of personal data is fully justifiable under the Data Protection Acts. Donegal Travellers Project should also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate.

6. Personnel who retire or resign etc. should be removed immediately from all mailing and email lists. Relevant changes should also occur when staff are transferred to other positions internally. It is the responsibility of Donegal Travellers Project to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual in a timely fashion.

7. Contractors, consultants and external service providers employed by Donegal Travellers Project should be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance.

8. Donegal Travellers Project has in place an up-to-date Acceptable Usage Policy in relation to the use of Information and Communications Technology (e.g. telephone, mobile phone, fax, email, internet, intranet and remote access, etc.) by staff members. This policy should be understood and signed by each user of such technology in Donegal Travellers Project.

9. Risks associated with the storage, handling and protection of personal data is included in the Donegal Travellers Project risk register and risk assessments and takes place as part of a Donegal Travellers Project risk strategy exercise.

10. Procedures have been put in place in relation to disposal of files (both paper and electronic) containing personal data. In doing so, Donegal Travellers Project need to be aware of their legal obligations as set out in the National Archives Act, 1986 and the associated National Archives Regulations, 1988. It should be noted that incoming and outgoing emails which are ‘of enduring interest’ are archivable records under the Act. Procedures should also be put in place in relation to the secure disposal of computer equipment (especially storage media) at end-of-life.

11. Individuals who use the services of Donegal Travellers Project should be aware on how each service user data is held and how it will be used/not used. Website privacy statements should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data.

12. New staff should be carefully coached and trained before being allowed to access confidential or personal files.

13. Staff should ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc.

14. All staff should ensure that PCs are logged off or ‘locked’ when left unattended for any period of time.

15. Personal and sensitive information should be locked away when not in use or at end of day.

16. Appropriate filing procedures (both paper and electronic) are drawn up and followed.

17. Donegal Travellers Project have to be aware of the care that needs to be adopted in the use of Personal Public Service Number (PPSN) in systems, on forms and documentation.

There is a strict statutory basis providing for the use of the PPSN. This allows the Donegal Travellers Project to use the PPSN in support of a provision of a public service to a service user. The Department of Social & Family Affairs manages the issuance and use of PPS Numbers.

PAPER RECORDS

The Data Protection Acts apply equally to personal data held on ICT systems and on paper files. The following guidelines should be followed with regard to personal and sensitive data held on paper files:-

1. Paper records and files containing personal data are handled in such a way as to restrict access only to those persons with business reasons to access them.
2. This entails the operation of a policy whereby paper files containing such data are locked away when not required.
3. Consideration is also be given to logging access to paper files containing such data and information items.
4. Personal and sensitive information held on paper needs to be kept hidden from callers to offices.

EMAIL AND PERSONAL PRODUCTIVITY SOFTWARE

Email and other personal productivity software such as word processing applications, spreadsheets, etc. are valuable business tools which are in use across the Donegal Travellers Project. However, Donegal Travellers Project must take extreme care in using this software where personal and sensitive data is concerned. In particular:-

1. Standard unencrypted email should **not** be used to transmit any data of a personal or sensitive nature. Departments that wish to use email to transfer such data must ensure that personal or sensitive information is encrypted through file encryption or through the use of a facility which will encrypt the data (including any attachments) being sent. Employees should also ensure that such email is sent only to the intended recipient.
2. Where personal or sensitive data is held on applications and databases with relevant security and access controls in place, additional controls should be considered that would prevent such data from being copied to personal productivity software (such as word

processing applications, spreadsheets, etc.) where no security or access controls are in place and/or can be bypassed.

REMOTE ACCESS

The demand from staff to access remotely the same systems that they can access from the office is increasing. This brings its own challenges in relation to data security which Donegal Travellers Project must address. With regard to personal and sensitive data, the following guidelines should be adhered to:-

1. In the first instance, all personal and sensitive data held electronically is stored by the individual team leader/staff member who needs the data and should not be copied to portable storage devices, such as laptops, memory sticks, etc. that may be stolen or lost;
2. Additional stringent security and access controls must be adopted by each user e.g. mandatory use of strong passwords.
3. Departments should ensure that only known machines (whether desktop PC, laptop, mobile phone, PDA, etc.) configured appropriately to the Donegal Travellers Project standards (e.g. with up-to-date anti-virus and anti-spyware software, etc.), are allowed to remotely access centrally held personal or sensitive data.
4. Staff should be aware that it is imperative that any wireless technologies/networks used when accessing the Department's systems should be encrypted to the strongest standard available

LAPTOPS AND OTHER MOBILE STORAGE DEVICES (INCL. MOBILE PHONES, PDAS, USB MEMORY STICKS, EXTERNAL HARD DRIVES, ETC.)

The use of laptops, USB memory sticks and other portable or removable storage has increased substantially in the last number of years. Likewise, the use of personal communications and storage devices such as mobile phones, PDAs, etc. has also increased. These devices are useful tools to meet the business needs of staff. They are, however, highly susceptible to loss or theft. To protect the content held on these devices, the following recommendations should be followed:

1. All portable devices should be password-protected to prevent unauthorised use of the device and unauthorised access to information held on the device. In the case of mobile phones, both a PIN and login password should be used. Manufacturer or operator-provided

PIN codes must be changed from the default setting by the user on receipt of the device;
2. Passwords used on these devices should be of sufficient strength to deter password cracking or guessing attacks. A password should include numbers, symbols, upper and lowercase letters. Password length should ideally be around 12 to 14 characters but at the very minimum 8 characters. Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided. Donegal Travellers Project must ensure that passwords are regularly changed.
3. Personal, private, sensitive or confidential data should not be stored on portable devices. In cases where this is unavoidable, all devices containing this type of data must be encrypted. With regard to laptops, full disk encryption must be employed regardless of the type of data stored.
4. With regard to mobile technologies, staff should be aware that when 'roaming' abroad, communications may not be as secure as they would be within Ireland.
5. Data held on portable devices should be backed up regularly to the Donegal Travellers Project's servers.
6. When portable computing devices are being used in public places, care must be taken to avoid unwitting disclosure of information, e.g. through overlooking or overhearing by unauthorised persons.
7. Portable devices must not contain unauthorised, unlicensed or personally licensed software.
8. Anti-virus/Anti-spyware/Personal Firewall software must be installed and kept up to date on portable devices. These devices should be subjected to regular virus checks using this software.
9. Donegal Travellers Project should ensure that when providing portable devices for use by staff members, each device is authorised for use by a specific named individual. The responsibility for the physical safeguarding of the device will then rest with that individual.
10. Laptops must be physically secured if left in the office overnight. When out of the office, the device should be kept secure at all times.
11. Portable devices should never be left in an unattended vehicle.
12. Portable storage media should only be used for data transfer where there is a business requirement to do so, should only be used on approved workstations and must be encrypted.
13. In order to minimise incidents of unauthorised access and/or incidents of lost/stolen data, Donegal Travellers Project should restrict the use of personal storage media and devices (e.g.

floppy disks, CDs, DVDs, USB memory sticks, etc.) to staff that require to use these media/devices for business purposes;
14. Staff owned devices such as portable media players (e.g. iPods, etc.), digital cameras, USB sticks, etc. must be technologically restricted from connecting to Donegal Travellers Project computers;
15. Donegal Travellers Project will implement procedures that will ensure that personal data held on mobile storage devices is fully deleted when the data is no longer required (e.g. through fully formatting the devices' hard drive);

DATA TRANSFERS

Data Transfers are a daily business requirement for Donegal Travellers Project. With regard to personal and sensitive data, such transfers should take place only where absolutely necessary, using the most secure channel available. To support this, Donegal Travellers Project core staff members should adhere to the following:-
1. Data transfers should, where possible, only take place via secure on-line channels where the data is encrypted rather than copying to media for transportation.

2. Manual data transfers using removable physical media (e.g. memory sticks, CDs, tape, etc.) should end where possible.
3. In the meantime, where data is copied to removable media for transportation such data must be encrypted using the strongest possible encryption method available. Strong passwords/passphrases (see 'General Procedures') must be used to encrypt/decrypt the data.
4. 'Strong' passwords (see 'General Procedures') must be used to protect any encrypted data. Such passwords must not be sent with the data it is intended to protect. Care should be taken to ensure that the password is sent securely to the intended recipient and that it is not disclosed to any other person.
5. Staff should ensure that such mail is sent only to the intended recipient.
6. When a data transfer with a third party is required (including to/from Government Departments), a written agreement should be put in place between both parties in advance of any data transfer. Such an agreement should define:-
· The information that is required by the third party (the purposes for which
the information can be used should also be defined if the recipient party is
carrying out processing on behalf of the organisation);

· Named contacts in each organisation responsible for the data;
· The frequency of the proposed transfers;
· An explanation of the requirement for the information/data transfer;
· The transfer method that will be used (e.g. Secure FTP, Secure email, etc.);
· The encryption method that will be used;
· The acknowledgement procedures on receipt of the data;
· The length of time the information will be retained by the third party;
· Confirmation from the third party that the information will be handled to the same level of controls that the Department apply to that category of information;
· Confirmation as to the point at which the third party will take over responsibility for protecting the data (e.g. on confirmed receipt of the data);
· The method of secure disposal of the transfer media and the timeline for disposal;
· The method for highlighting breaches in the transfer process;
· For data controller to data controller transfers (as opposed to a data controller to a data processor transfer), it needs to be clear that only necessary data is transferred to meet the purposes;
· Business procedures need to be in place to ensure that all such transfers are legal, justifiable and that only necessary data is transferred to meet the purposes;

APPROPRIATE ACCESS AND AUDIT TRAIL MONITORING

All organisations have an obligation to keep information 'safe and secure' and have appropriate measures in place to prevent "unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction" in compliance with sections 2(1)(d) and 2C of the Data Protection Acts 1988 & 2003.
It is imperative, therefore, that Donegal Travellers Project has security in place to ensure that only those staff members with a business need to access a particular set of personal or sensitive data are allowed to access that data. In addition to this general requirement, the following guidelines should be followed:-
1. Donegal Travellers Project must ensure that their ICT systems are protected by use of appropriate firewall technologies and that this technology is kept up-to-date and is sufficient to meet emerging threats.
2. In order to capture instances of inappropriate access (whether internal or external), addition, deletion and editing of data, audit trails should be used where technically possible.

3. Access to files containing personal data is monitored by the Project Manager on an ongoing basis. Staff should be made aware that this is being done. IT systems will be put in place to support this supervision.

BREACH MANAGEMENT

A data security breach can happen for a number of reasons, including:-

· Loss or theft of data or equipment on which data is stored (including break-in to an organisation's premises);
· Inappropriate access controls allowing unauthorised use;
· Equipment failure;
· Human error;
· Unforeseen circumstances such as a flood or fire;
· A hacking attack;
· Access where information is obtained by deceiving the organisation that holds it.

It is important that Donegal Travellers Project incorporate a breach management plan to follow should such an incident occur. There are five elements to any breach management plan:-

1. Identification and Classification
2. Containment and Recovery
3. Risk Assessment
4. Notification of Breach
5. Evaluation and Response

1. Identification and Classification

Donegal Travellers Project have in place procedures that allow any staff member to report an information security incident. It is important that all staff are aware to whom they should report such an incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner. Details of the incident must be recorded accurately, including the date and time the incident occurred, the date and time it was detected, who/what reported the incident, description of the incident, details of any ICT systems involved, corroborating material such as error messages, log files, etc. In this respect, staff need to be made fully aware as to what constitutes a breach.

2. Containment and Recovery

Containment involves limiting the scope and impact of the breach of data protection procedures.

If a breach occurs, Donegal Travellers Project will:-

· decide on who would take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;

· establish who in the organisation needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network, finding a lost file or piece of equipment, etc.;

· establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;

· where appropriate, inform the Garda.

3. Risk Assessment

In assessing the risk arising from a data security breach, Donegal Travellers Project will consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be.

In assessing the risk, Departments should consider the following points:-

· what type of data is involved?

· how sensitive it is?

· are there any protections in place (e.g. encryption)?

· what could the data tell a third party about the individual?

· how many individuals' personal data are affected by the breach?

4. Notification of Breaches

Although there is no current explicit legal obligation to notify individuals or other bodies under the Data Protection Acts of a breach, the Data Protection Commissioner's Office encourages voluntary notification and early engagement with the Office. Therefore, if inappropriate release/loss of personal data occurs it should be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is. In this regard, Donegal Travellers Project should be aware of the dangers of 'over notifying'. Not every incident will warrant notification.

When notifying individuals, Donegal Travellers Project should consider using the most appropriate medium to do so. They should also bear in mind the security of the medium used for notifying individuals of a breach of data protection procedures and the urgency of the situation. Specific and clear advice should be given to individuals on the steps they can take to protect themselves and what the Donegal Travellers Project is willing to do to assist them. Donegal Travellers Project should also provide a way in which individuals can make contact for further information, e.g. a helpline number, webpage, etc.

Donegal Travellers Project will consider notifying third parties such as the Garda, bank or credit card companies who can assist in reducing the risk of financial loss to individuals. The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

5. Evaluation and Response

Subsequent to any information security breach a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved. Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter. Donegal Travellers Project will identify an individual within the organisation who will be responsible for the control of actions to reported breaches of security.