DCSD 011 - Data Protection Policy

Policy Statement

DCSD Community Pilgrimage

DCSD Community Pilgrimage to Lourdes

Policy Statement

DCSD 011 – Data Protection Policy

Pilgrimage Director Mr Dominic Pew

Created May 2018

Information Reader	
Document Purpose	Information & Guidance
Document Name	Data Protection Policy
First Publication Date	5th May 2018
Target Audience	Anyone who shares information with the DCSD
Additional Circulation List	Not Applicable
Description	This policy describes how personal data is collected, handled and stored to meet the organisations data protection standards — and to comply with the law.
Cross Reference	**DCSD012 -** Privacy Policy **DCSD013 -** Social Media Policy **DCSD014 -** Website Terms and Conditions **DCSD015 -** Cookie Policy
Superseded document	Not Applicable
Author	Dominic Pew

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy.

Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

All DCSD Community Pilgrimage policies and procedures can be found on out downloads page of our website https://www.dcsdcommunitypilgrimage.org/policies-and-procedures

Document Number: DCSD011	Issue Date: 5th May 2018	Version Number: 1.0
Status: Live Controlled Document	Next review date: 4th May 2019	

Introduction

The DCSD Community Pilgrimage needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the organisations data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures The DCSD Community Pilgrimage:

- Complies with data protection law and follow good practice
- Protects the rights of trustees, volunteers and pilgrims
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including The DCSD Community Pilgrimage— must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to:

- The head office of The DCSD Community Pilgrimage
- All trustees and volunteers of The DCSD Community Pilgrimage
- All contractors, suppliers and other people working on behalf of The DCSD Community Pilgrimage

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Medical information
- Any other information relating to individuals

Data protection risks

This policy helps to protect The DCSD Community Pilgrimage from some very real data security risks, including:

- Breaches of confidentiality.
    - For instance, information being given out inappropriately.
- Failing to offer choice.
    - For instance, all individuals should be free to choose how the organisation uses data relating to them.
- Reputational damage.
    - For instance, the organisation could suffer if hackers successfully gained access to sensitive data.

Responsibilities

All members of the DCSD Community Pilgrimage have some responsibility for ensuring data is collected, stored and handled appropriately.

Anyone who handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The pilgrimage director is ultimately responsible for ensuring that The DCSD Community Pilgrimage meets its legal obligations which include:

- Keeping the trustees updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from trustees, volunteers and anyone else covered by this policy.
- Dealing with requests from individuals to see the data The DCSD Community Pilgrimage holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the organisation is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- To ensure marketing initiatives abide by data protection principles.

General guidelines

- The only people able to access data covered by this policy should be those who are authorised by the trustees and the person the information relates to.
- Data should not be shared informally. When access to confidential information is required, volunteers or organisations can request it from the pilgrimage director.
- The DCSD Community Pilgrimage will provide training to trustees and volunteers to help them understand their responsibilities when handling data.
- Trustees and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.
    - In particular, strong passwords must be used and they should never be shared.
    - Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
    - Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    - Trustees or volunteers should request help from the pilgrimage director if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the pilgrimage director.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Trustees and volunteers should make sure paper and printouts are not left where unauthorised people could see them.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the organisations standard backup procedures.
- Data should never be saved directly mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security Software and a firewall.

Data use

Personal data is of no value to The DCSD Community Pilgrimage unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, trustees and volunteers should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Trustees and volunteers should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

Data accuracy

The law requires The DCSD Community Pilgrimage to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort The DCSD Community Pilgrimage should put into ensuring its accuracy.

It is the responsibility of all trustees and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Trustees and volunteers should not create any unnecessary additional data sets.
- Trustees and volunteers should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The DCSD Community Pilgrimage will make it easy for data subjects to update the information The DCSD Community Pilgrimage holds about them. For instance, via the organisations website company website.
- Data should be updated as inaccuracies are discovered. For instance, if a pilgrim or volunteer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by The DCSD Community Pilgrimage are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the organisation requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the pilgrimage director at director@dcsdcommunitypilgrimage.org. The pilgrimage director can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The pilgrimage director will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, The DCSD Community Pilgrimage will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the organisations legal advisers where necessary.

Providing information

The DCSD Community Pilgrimage aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the organisation has a privacy statement, setting out how data relating to individuals is used by the organisation.