Shepherds Dene
retreat house

May 2018

GDPR Policy

Shepherds Dene Retreat House (The Stirling Newall Trust)

On 25th May 2018 the UK and EU the law on data protection will change, giving people more say in their relationship with organisations who hold their personal details. We have updated our data policies to comply with these changes and set out how we use the information we hold. Please be assured that your details are safe with us and we will never share them with anyone else.

Shepherds Dene has adopted three policies that relate to data privacy and how we handle your data:

- Privacy Policy – outlines our commitment to you concerning your personal data.
- Data Retention Policy –outlines the different types of personal data we hold and the period of time we will hold them for.
- GDPR Policy – this policy outlines, in practical terms, how we comply with GDPR and PECR, and details of how we manage 'Consent' and where we use 'Legitimate Interest' to contact individuals and representatives of organisations.

What data do we hold?

Staff: names, addresses, bank details, national insurance numbers, age, date of birth, salary and income details, payslips, sick notes from GPs, for example.

Guests: names, addresses, telephone numbers, e-mail addresses, dietary and mobility requirements, bank account details (occasionally), bank card numbers (on card machine printouts)

Trustees: names, addresses, telephone numbers, e-mail addresses, dates of birth, personal details (colour of eyes)

Volunteers/friends: names, addresses, telephone numbers, bank account details

Suppliers: organisation and individual names, addresses, bank account details

Photos: some digital photos of guests and staff who have given consent in the past

Where do we receive data from?

Staff: Application Forms

New starter Employee Forms

Contact Detail Forms

Payslips from accountants

GPs (medical sick notes etc)

Occupational Health

Gift Aid donations

Guests: Direct from guests who make bookings – verbally, by letter and by e-mail.

Booking forms, via the Shepherds Dene website

Our own historical records, google diary and mailing lists for marketing purposes.

Suppliers: Electronic communications, paper documents, verbally

Who do we share data with and why?

Accountants: for processing payroll purposes

Trustees: for communicating directly with employees, guests, friends/volunteers

Internally: for information about visiting guests for staff and for health and safety/fire regulations.

Bank: payments by cheque paid into bank would have bank account details and sort codes.

Pension organisations (company pension of individual's private pension)

Online accounting software (names of customers and suppliers)

Online banking: bank account and sort code details and other data in order to process payments from guests, employees and suppliers.

How do we store data and for how long?

Paper files and records (archived in storage containers in locked cellar):

- archive materials relating to the history of the house (back to 1946)
- financial and operational records – 10 years.
- Paperwork relating to employment: 3 years after employment ceases.

Computer records:

- e-mails: 3 years
- Online electronic mailing list: until guests or contacts ask for their details to be removed (having requested to be included on the mailing list in writing) or until correspondence from Shepherds Dene for confirmation of data is received.
- Personal data stored on shared network in the admin office (4 workstations) but is not accessible by anyone other than named staff and trustees and then, is password protected.

On what basis does Shepherds Dene process personal data?

Legitimate Interest ground:

- processing personal is necessary for the purposes of the legitimate interest pursued in the day to day operations of the organisation (staff, suppliers, guests, volunteers/friends and trustees)
- the data subjects have all given their consent in the past (staff, suppliers, guests, volunteers/friends and trustees)
- processing of data is necessary for contracts to be performed (bookings, supplies and deliveries, payroll)
- We are legally obliged to keep details for trustees, employees and volunteers/friends and those who donate through Gift Aid.

Consent ground:

- guests who give their personal details for mailing list and e-bulletin have done so by completing forms in the office or front of house, on feedback forms, by e-mail.
- As previous consent (see above) complies with the new requirements, new consent will not be required.

Contractual ground:

- Employees and trustees are party to contracts with Shepherds Dene.
- Guests, visitors and suppliers are also party to entering into a contract with Shepherds Dene.

Special categories of personal data:

- Shepherds Dene keeps certain details relating to medical conditions, dietary requirements and mobility requirements of guests as they are required for safeguarding purposes and the general operation of the organisation.
- Shepherds Dene keeps records of staff medical conditions when not fit for work and in relevant archives for the required length of time.

How will Shepherds Dene ensure compliance prior to and after the 25th May 2018?

Shepherds Dene Retreat House will ensure robust systems are in place to meet the legal requirements of data protection legislation from 25th May 2018. We will introduce new measures for obtaining consent, for storing personal data and for the sharing of personal data. Privacy policies and data retention policies for suppliers, guests, employees and volunteers will be in place from 25th May 2018 and all staff and trustees will be made aware of the changes.

The rights of an EU resident under the GDPR, and how you can exercise those rights with respect to Shepherds Dene Retreat House, are as follows:

- **Right of access:** you can ask us what personal data is being processed (used), why and where.
- **Right to rectification:** you may correct, revise or remove any of the data we retain on you - as explained in our privacy statement (see our website)- you may do so at any time.
- **Right to be forgotten:** if you wish your personal data to be removed from our system at any time, we will permanently remove your data and all information associated with it.
- **Right to restrict processing:** If you believe your personal data is inaccurate or collected unlawfully, you may request limited use of your personal data.
- **Right of portability:** We provide you with the ability to move any of your data to a third party at any time.
- **Right to object:** If you decide that you no longer wish to allow your data to be included in our analytics or for us to provide personalised (targeted) marketing content and information relating to Shepherds Dene at any time, you may contact us to request removal of this data.

Ensuring policies and Procedures are up to date

Trustees of Shepherds Dene Retreat House have a duty to keep policies and procedures up to date. Changes to policies and procedures are submitted to trustees at one of the quarterly trustees' meetings for approval.

Data Protection Impact Assessment Procedure

A Data Protection Impact Assessment (DPIA) is a process to help us to identify and minimise the data protection risks of a project.

Trustees must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. We can use screening checklists to help you decide when to do a DPIA.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

Our DPIA will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

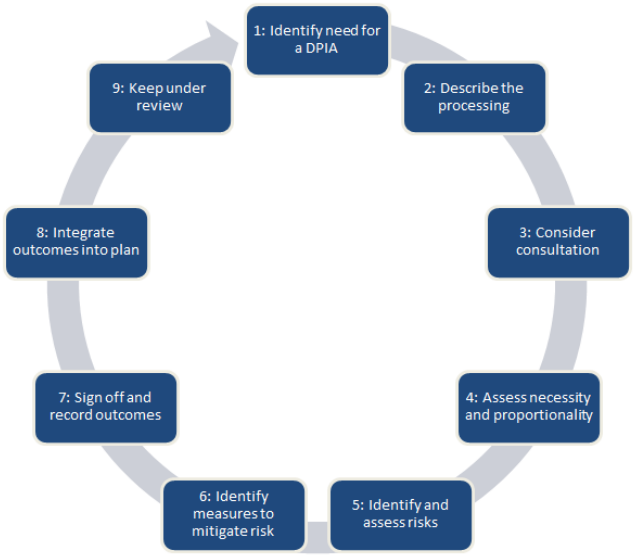
To assess the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We should consult our data protection officer (if we have one) and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.

If we identify a high risk that we cannot mitigate, we must consult the ICO before starting the processing.

The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data or ban the processing altogether.

A full checklist for DPIA procedure is attached in Appendix 1 on page 7.



What systems are in place to allow new rights of individuals to be satisfied?

Data Protection Policies, Notices and Retention Policies have been updated to ensure compliance with changes in the law from 25th May 2018.

New policies include the 6 rights as identified by the EU regarding the protection of personal data.

Policies are published on the company's website, along with contact information for withdrawing consent or for making a complaint.

Customers are invited to complete forms to give consent for marketing and information purposes in the future.

Passwords have been introduced onto all admin workstations.

Staff personal data on paper is stored in locked filing cabinet.

The administration office will always be locked if there is no member of staff present.

Staff and trustees have been made aware of the change in the law and made aware of the introduction of new policies.

Record Keeping:

As an organisation with less than 250 employees Shepherds Dene is not required to carry out the detailed record keeping unless:

It is likely to result in risk to rights and freedoms of data subjects

It is not occasional

It includes special categories of data or personal data relating to criminal convictions and offences.

Who will take the lead on Data Protection within Shepherds Dene?

As a small organisation which does not carry out large scale systematic monitoring or criminal convictions and sensitive data, Shepherds Dene is not required to nominate a Data Protection Officer.

The trustees have responsibility for ensuring compliant policies and procedures are in place and the Director has responsibility, along with trustees, for the implementation of said policies and procedures.

Appendix 1

DPIA awareness checklist

We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

Our existing policies, processes and procedures include references to DPIA requirements.

We understand the types of processing that require a DPIA, and use the screening checklist to identify the need for a DPIA, where necessary.

We have created and documented a DPIA process.

We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

We always carry out a DPIA if we plan to:

- Use systematic or extensive profiling or automated decision-making to make significant decisions about people.
- Process special category data or criminal offence data on a large scale.
- Systematically monitor a publicly accessible place on a large scale.
- Use new technologies.
- Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit.
- Carry out profiling on a large scale.
- Process biometric or genetic data.
- Combine, compare or match data from multiple sources.
- Process personal data without providing a privacy notice directly to the individual.
- Process personal data in a way which involves tracking individuals' online or offline location or behaviour.
- Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them.
- Process personal data which could result in a risk of physical harm in the event of a security breach.

We consider whether to do a DPIA if we plan to carry out any other:

- Evaluation or scoring.

- Automated decision-making with significant effects.
- Systematic
- Processing of sensitive data or data of a highly personal nature.
- Processing on a large scale.
- Processing of data concerning vulnerable data subjects.
- Innovative technological or organisational solutions.
- Processing involving preventing data subjects from exercising a right or using a service or contract.
- We consider carrying out a DPIA in any major project involving the use of personal data.
- If we decide not to carry out a DPIA, we document our reasons.
- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

DPIA process checklist

We describe the nature, scope, context and purposes of the processing.

We ask our data processors to help us understand and document their processing activities and identify any associated risks.

We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

We ask for the advice of our data protection officer.

We check that the processing is necessary for and proportionate to our purposes and describe how we will ensure data protection compliance.

We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

We identify measures we can put in place to eliminate or reduce high risks.

We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

We implement the measures we identified and integrate them into our project plan.

We consult the ICO before processing, if we cannot mitigate high risks.

We keep our DPIAs under review and revisit them when necessary.