Data Protection Policy

This policy applies to all employees within Parkwood Leisure Holdings Ltd, Alston Investments Ltd, their respective subsidiaries and Parkwood Managed Companies.

Parkwood House
Preston

Telephone: 01772 627111

Document Status

Issue	Reason for change	Date	Actioned by
1.1	New policy	16.09.10	Carolyn Stockdale
	Amended Sept 2011		Graham Airey
			Sue McGrath
2.1	Amendment following review and lessons learned	07.10.14	Graham Airey Alan Tucker
2.2	Amendment following changes to organisation structure and DPO's.	16.02.16	Graham Airey Rebecca Coombes
2.3	Amendment regarding paper storage	23.08.16	Graham Airey
2.4	GDPR update	26.01.18	Graham Airey

Related Documents

Version	Reference	Name	Date
	HR028	Records Management Policy	
		Disciplinary Policy	
	ITP001	IT Acceptable Use Policy	
		Employee Handbook	
		Induction	
		Employee Form	
	ITP004	Data Security Breach Management Policy	
	ITF006	Data Breach Report Form	

1. Introduction

The Company ("**Parkwood Leisure Holdings Ltd, Alston Investments Ltd, and their respective subsidiaries and Parkwood Managed Companies**") is fully committed to compliance with the requirements of the Data Protection Act 1998 (the "Act") and the General Data Protection Regulation (effective 25/5/18) and will therefore follow procedures that aim to ensure that all employees, contractors, agents, consultants or other individuals who have access to any personal data held by or on behalf of the Company, are fully aware of and abide by their duties and responsibilities under the Act.

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

2. Statement of policy

In order to operate efficiently, the Company have to collect and use personal information about people with whom it works and provides services to. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, regardless of how it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

The Company regards the lawful and correct treatment of personal data as very important to its successful operations and to maintaining confidence between the Company and those with whom it carries out business. The Company will ensure that it treats personal information lawfully and correctly.

To this end, the Company endorses and adheres to the Principles of Data Protection as set out in the Act.

3. Handling of personal data

The Company will, through appropriate management and the use of strict criteria and controls:-

- observe fully conditions regarding the fair collection and use of personal data;
- only obtain and process personal data by lawful and fair means;
- use non-identifiable information wherever possible and limit the collection of personal data to that necessary to accomplish a legitimate business purpose;
- collect and process appropriate personal data and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of personal data used;
- ensure that valid consent is sought (see Appendix B);
- adhere to the Records Management policy detailing the length of time employee personal data is held;

- take appropriate technical and organisational security measures to safeguard personal data;
- ensure that the rights of people about whom the personal data is held can be fully exercised under the Act.

  These rights include:

  - The right to be informed that processing is being undertaken
  - The right to receive a copy of their own personal data within one month;
  - The right to prevent processing in certain circumstances;
  - The right to correct, rectify, block or erase personal data regarded as wrong data.

4. The principles of data protection

The Act stipulates that anyone processing personal data must comply with the eight principles of good practice. These principles are legally enforceable.

The principles require that personal data is:

- Fairly and lawfully processed;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than necessary;
- Processed in line with the individual's rights;
- Secure;
- Not transferred to other countries without adequate protection.

The Act provides conditions for the processing of any personal data.

Personal data is defined as data relating to a living individual who can be identified from:

that data and other information which is in the possession of, or is likely to come into the possession of the Company; and includes any expression of opinion about the individual and any indication of the intentions of the Company, or any other person in respect of the individual. Examples of such information are:

- Personnel Records
- Membership databases
- Client mailing lists
- Individual customer data cards (e.g Loyaltee , Expressions)
- Job Applications
- Crèche Records

This list is an example of the type of information referred to. In reality the information required to be protected is any information where an individual's personal data can be identified.

5. Roles and responsibilities

5.1 All Employees

Employees are responsible for:

- Ensuring that any personal data provided in connection with their employment is accurate and up to date;
- Notifying the Company in writing if this data changes to ensure personal data provided is accurate and up to date, for example, change of address, name etc;
- Ensuring they are familiar with and follow this policy and the eight data protection principles at all times.
- Ensuring that if they have access to any other individual's personal data, that they do not provide that information to any third party without the consent of the individual.

5.2 Data security

Employees are also responsible for ensuring that any personal data, whether in electronic or paper format, is held and processed securely including:

- Appropriate password/screensaver protection is in place prior to going home or leaving a workstation for any length of time.
- Not disclosing passwords to anyone.
- A suitable secure environment is in place for the storage of personal data on portable disks/manual records. This includes using lockable filing cabinets for all paper based documents containing personal data.
- Personal data should not be held locally on staff devices such as PC's or laptops.
- Personal data is not disclosed by any medium, accidentally or otherwise, to any unidentified or unauthorised third party.

If an employee is in any doubt about what they may or may not do under data protection legislation, they must seek advice from their Manager. If the employee cannot get in touch with their manager, then they must not disclose any personal data.

Failure on the part of any employee to comply with any of the requirements set out in this policy and associated guidance is a disciplinary offence and may result in disciplinary action. In some cases this could result in dismissal and may also lead to a criminal prosecution

It should be noted that the provision of personal data to a third party by an employee is not only associated with work activities. If an employee is found in any other capacity to have provided information which it may reasonably be considered had been obtained from the workplace then although the company is not responsible for their actions, the Company will take disciplinary action against the employee. The employee should also recognise that they personally may be subject to criminal and civil proceedings taken by the third party. An example of such a situation is posting personal data on social media sites such as Facebook, Google+ and Twitter.

5.3 All Managers

In addition to the above, all Managers are responsible for ensuring:

- Their direct reports are aware of the employee's obligations under the Act, this policy and of any local security protocols/requirements for the holding and processing of personal data (including any other users of the Company's information systems that they are responsible for);

- Any personal data they hold for day to day operational management purposes (for example, notes that may be needed) is kept to a minimum, processed for a specific purpose and held confidentially in accordance with the eight data protection principles;
- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computer systems is protected by the use of individually allocated secure passwords;
- Individual passwords are not easily compromised.
- That all employees identified as having access to personal data receive the required awareness training of the requirements of data protection and sign to say they understand their responsibilities. Any employee failing to carry out awareness training and signing to say they have will not be given access to systems containing personal data and will therefore in some cases not be capable of performing their role.

5.4 All Employees who have Human Resources responsibilities

In addition to the above, all employees who have Human Resources responsibilities and handle employee personal data are responsible for:

- Limiting internal access to HR records to authorised users only (i.e. on the need to know principle, by restricting confidential personal data only to those who need to have access in order to carry out their duties/role effectively. Other designated employees with a legitimate need are also granted access as appropriate);
- Verifying employee identification prior to facilitating personal data requests;
- Holding all manual HR records confidentially and securely in lockable storage (which is only left open during normal office hours).
- Ensuring files leaving an area are booked in and out by an authorised employee.
- Ensuring that all employee databases i.e payroll are password protected and that the individual password is not given to any other person

Examples of staff who have these responsibilities are Line Managers, Human Resources Personnel, Administrators.

5.5 All contractors, consultants or other servants or agents of the Company must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Company, are aware of this policy and confirm that they are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the Company and that individual, company, partner or firm;
- Allow data protection audits by the Company of personal data held on its behalf (if requested);
- Indemnify the Company against any costs arising from prosecutions, claims, proceedings, actions or payments of compensation or damages without limitation.

All contractors who may have access to personal data supplied by the Company will be required to confirm that they will abide by the requirements of the Act with regard to data supplied by the Company.

6. Disclosure requirements from and to external organisations

- Disclosure requests are requests made from third parties to the Company for information about employees containing personal data, and or for information on personal data relating to information held on any individual.
- Personal data relating to an employee will not be disclosed to a third party without the consent of the employee, unless the disclosure is permitted by law under statute or is necessary for the prevention or detection of crime (Examples are the Police, Local Authority Safeguarding, Social Services etc).
- Where a request by a third party for disclosure is made, which requires the consent of the employee to be given, then the employee must be informed as soon as is practicable and their consent obtained, unless the Company is prevented by law from doing so or if obtaining consent would prejudice a criminal or tax investigation. Where a disclosure request is received, the identity and the authority of the person/organisation making it will be verified before any disclosure is made.
- Where a request by a third party for disclosure is made for personal data held on any individual other than an employee the information will not be provided unless the disclosure is permitted by law under statute or is necessary for the prevention or detection of crime (Examples are the Police, Local Authority Safeguarding, Social Services etc).

7. Direct Marketing

Is defined as, contact via the use of personal data regarding the activities/products/ services of the Company which involves the processing of personal data, e.g. someone's name, address or email address.

It is prohibited to send marketing email, text or other social media messages without prior consent unless there is an existing relationship between the Company and the recipient.

- **Email** – in all instances of direct email marketing activities' recipients must be given a clear, distinct and simple means of refusing (free of charge except for the cost of the transmission of the refusal) the use of his/her contact details for the purpose of such direct marketing on each occasion the direct marketing takes place.
- **Text** – The same rules as email marketing apply to the use of text messaging for direct marketing purposes.
- **Telephone** – (whether by voice or fax). It is prohibited to make unsolicited calls for direct marketing purposes where the number called is that of a subscriber who has previously notified Parkwood that such calls should not be made, or has been entered on a specific register maintained for that purpose. In the UK the register of numbers is maintained by the Telephone Preference Service.
- **Social Media** - The same rules as email marketing apply to the use of social media messaging for direct marketing purposes

8. Information Technology

8.1 IT Acceptable Use Policy

All Company employees should ensure that they are fully aware of, and have signed a copy of the IT Acceptable Use Policy.

8.2 Security

Only authorised Company employees should access, alter, disclose or destroy personal data (this includes both internal and external IT solutions such as Google GSuite, Legend, Spektrix, Passfield, Loyaltee and ADP). These employees should only act within the scope of their authority, and it is Company policy that any breach of any of the obligations will be treated extremely seriously and will result, not only in disciplinary action, but also in certain cases in legal action against the employee.

9. Company E-mail Addresses

The Company reserves the right to use email addresses provided by the company for the distribution of information relating to the company or any benefits, such as discount schemes with third parties that have been negotiated by the company on the employee's behalf.

10. Personal Email Addresses

The Company will allow employees via a specific consent form to provide their email addresses for the company to use for the distribution of information relating to the company news and marketing and to have specific employment related correspondence emailed to them.

The Parkwood Group will ensure that;

- Only the information described above will be sent to employees via their personal email addresses.
- Everyone who has access to personal email addresses has a genuine need.
- Employees who have access to personal email addresses will be regularly reviewed to sure only relevant staff have access.
- Employees can opt out of receiving information from the company to their personal email address at any point.

11. Use of Employee Photographs

The Company reserve the right to use photographs taken in the course of employment for the promotion of the company except where an individual expressly requests for them not to be used.

12. Photographing of members of Vulnerable Groups including Children

The taking of photographs using videos, photographs, and mobile phones is expressly forbidden without the formal authorisation and evidence of authorisation as set out in the procedures for taking photographs.

13. Additional Responsibilities

The Company will ensure that:

- There is someone with specific nominated responsibility for data protection in the organisation;
- Everyone accessing and handling personal information is appropriately trained to do so;
- Anyone wanting to make enquiries about personal data, whether a member of staff of a member of the public, knows what to do;
- Queries about personal data are promptly and courteously dealt with;
- Methods of accessing and handling personal data are regularly assessed and evaluated;
- Data Protection policies and processes are reviewed and audited.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

14. Implementation

Senior management will be responsible for instigating the implementation of this policy throughout the Company. The Company will ensure that:

- Sufficient data protection training is provided, for employees who are accessing and using personal data within the Company, and that these individuals signed to say that they do understand their responsibilities in relation to Data Protection of Personal Data.;
- Best practice guidelines are followed;
- That all subsidiary Companies ensure they have relevant policies and procedures in place to ensure protection of personal data in relation to the specific process and databases they have,
- Compliance checks are conducted to ensure adherence, throughout the company, with the Act.

15. Notification of a Breach

If there is a potential breach of this policy then it should be reported via the ITF006 Data Breach Report Form. The guidance within the ITP004 Data Security Breach Management Policy would then be followed.

16. Notification to the Information Commissioner

The Information Commissioner (ICO) maintains a public register of data controllers, and the appropriate companies are registered as such.

The Act requires most data controllers that process data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. To this end each Managing Director will be responsible for notifying and updating the Information Commissioner of the processing of personal data, for their company.

Each Managing Director will review the Data Protection registration annually, prior to notification to the ICO.

Any changes to the registration will be notified to the ICO within 28 days.

To this end, any changes made between reviews must be brought to the attention of the Managing Director immediately.

Appendix A - Definitions of terms used in the Act and interpreted in the policy

Data Controller
The person or team who decides what personal information the Company will hold and how it will be held or used. In this instance, the Company is the Data Controller under the Act. It is also responsible for notifying the Information Commissioner's Office (ICO) of the data it holds, or is likely to hold and the general purposes that the data will be used for. This is reviewed annually as part of the registration process with the ICO.

Data Subject
The individual whose personal information is being held or processed by the Company, for instance: person with Company, person affected by the Company, employee, volunteer, etc.

Personal Data/Information
Information that relates to a living person (e.g. name and address). The Data Protection Act principles do not relate to deceased people, however the Company would need to carry out an assessment of any other obligations, legal or otherwise, towards any deceased person before using their information in any way.

Sensitive Data/Information
This includes:
o Racial or ethnic origin
o Political opinions
o Religious or similar beliefs
o Trade union membership
o Physical or mental health
o Sexual life
o Criminal record
o Criminal proceedings relating to an Individual's offences.

Appendix B - Gaining Consent

Under GDPR, a lawful basis needs to be identified before personal data can be processed. If there is no other lawful purpose identified, then consent must be sought.

To be considered a lawful basis to process data one of the following must apply:

- Processing is necessary for the performance of a contract with the Data Subject, or to take steps to enter a contract. This could be to fulfil an employment contract, or a contract to provide goods or services.
- Processing is necessary to comply with a legal obligation
- Processing is necessary to protect the vital interests of a Data Subject or another Person
- Processing is necessary to fulfil a task that is in the public interest or in the exercise of official authority vested in the Data Controller
- Processing is necessary for the purposes of legitimate interests of the Company and those legitimate interests are not outweighed by possible harm to the Data Subject's rights and interests
- Processing of data has consent from the Data Subject.

What is valid consent?

Consent must be:

- Freely given: the Data Subject has choice and control on how their personal data may be used
- Specific and informed: the Data Subject understands all the purposes for which their data may be used. If there are multiple purposes, consent must be sought for each
- Unambiguous: the Individual knows what they have consented to, and that they have given their consent
- A deliberate action by the Data Subject e.g. signing / verbal / electronic binary choice options.
- Consent may be implied, for example when completing a survey. The personal data provided may be used for the purposes stated in the survey. The data may not be used for any other purpose unless specific consent has been asked and an action has been taken to indicate it has been given.

Consent may provide a 'soft opt-in' for further contact. For example details may be captured to
provide a service and it would be reasonable to send details about similar services as long as there is the ability to opt-out every time there is contact.

Obtaining, recording and managing consent

Consent must be clearly distinguishable from other matters, written in an accessible and intelligible form and in clear and plain language.

It must be clear who has consented, when the consent was given, how it was given, what was consented to (it may be appropriate to note which version of the privacy notice was in use at the time) and when the Data Subject withdrew consent.

Consent is likely to degrade over time. If there is still interaction with the Data Subject renewed
consent will not be necessary. However if the processing or purposes the personal data is used
for changes then the original consent may not be specific enough.