DATA PROTECTION POLICY

Kings Lynn BID Limited trading as Discover Kings Lynn ("Discover Kings Lynn") is committed to ensuring its compliance with the requirements of the Data Protection Act 1998 (the **Act**). We recognise the importance of personal data to our business and the importance of respecting the privacy rights of individuals. This Data Protection Policy (the **Policy**) sets out the principles which we will apply to our processing of personal data so that we not only safeguard one or our most valuable assets, but also respect the data protection rights of individuals and process their personal data in accordance with the law.

It is the responsibility of all Discover Kings Lynn staff (which term includes contractors, temporary and permanent employees) to assist Discover Kings Lynn to comply with this Policy. In order to help staff to comply with this Policy, we have produced a Data Protection Guidance document (the **Guidance**) which explains in more detail the requirements of the Act. All staff must familiarise themselves with both this Policy and the Guidance and apply their provisions in relation to all processing of personal data. Failure to do so could amount to misconduct, which is a disciplinary matter and could ultimately lead to dismissal. Serious breaches could also result in personal criminal liability under the Act.

In addition, a failure to comply with this Policy could expose the business to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data and/or the imposition of monetary penalties) and to complaints or claims for compensation from affected individuals. There may also be negative publicity as a result of any breach that is made public.

For these reasons, it is important that all staff familiarise themselves with this Policy and the Guidance, and attend all training sessions in respect of the care and handling of personal data.

Data protection principles

Discover Kings Lynn will comply with the following principles in respect of any personal data which it processes as a data controller:

1 Personal data must be processed fairly and lawfully and must not be processed unless:

1.1 at least one of the conditions in Schedule 2 to the Act is met; and

1.2 in the case of sensitive personal data, at least one of the conditions in Schedule 3 to the Act is also met.

The Schedule 2 and 3 conditions are set out and explained in the Guidance.

2 Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

3 Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data must be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data must be processed in accordance with the rights of data subjects under the Act. These rights are:

6.1 the right of subject access;

6.2 the right to prevent processing likely to cause damage or distress;

6.3 the right to prevent processing for purposes of direct marketing;

6.4 the right to object to automated decision-taking.

7 Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This Policy may be amended from time to time to reflect any changes in legislation. Any queries should be directed to the Data Protection Officer

October 2017

DATA PROTECTION POLICY

GUIDANCE NOTE

INTRODUCTION

This Guidance Note (the Guidance) forms part of the Data Protection Policy and provides supplementary information to enable staff (which term includes temporary and permanent employees, contractors, agency staff) to better understand and comply with the Data Protection Policy.

King's Lynn BID Limited is required to comply with the Data Protection Act 1998 (the Act) in respect of its processing of personal data (such as information about our customers, employees and suppliers). It is important for all members of staff to familiarise themselves with both the Data Protection Policy and this Guidance so that any processing of personal data can be carried out in accordance with the Act. Failure to do so may expose King's Lynn BID Limited to enforcement action by the Information Commissioner (which could result in restrictions being imposed on our use of personal data and/or the imposition of monetary penalties) and/or to complaints and/or claims for compensation from affected individuals. There may also be negative publicity as a result of a breach.

You are required to assist King's Lynn BID Limited to comply with its obligations under the Act. In order to do this you must comply with the Data Protection Policy and this Guidance whenever you process personal data, as well as any other data protection related policy that may be applicable to your area of work. Any failure to comply with this policy may be a disciplinary offence which could result in dismissal. Negligent or deliberate breaches could result in criminal liability for you personally under the Act.

Any questions about the Data Protection Policy or this Guidance should be raised with the Data Protection Officer

References in this Guidance to **we** and **our** refer to King's Lynn BID Limited trading as Discover Kings Lynn and **you** refers to members of staff.

LEGAL FRAMEWORK

The Act sets out eight data protection principles which must be followed in relation to all processing of personal data. These principles are set out in the Data Protection Policy and are reproduced below, together with an explanation of what they require.

King's Lynn BID Limited processes personal data about a wide range of data subjects, such as employees, customers, members, and suppliers. We process personal data for a number of purposes, such as personnel administration, payroll, customer administration, marketing, profiling our customers, statistical analysis and credit checking. It is critical to our business that we are able to use personal data in this way. In order to continue to be able to do so, we must ensure compliance with the principles set out in the Act.

DEFINITIONS

In order to fully appreciate the requirements of the Act it is important for you to understand the meaning of certain key words and phrases which are used within the Act. These are set out below:

Data	is information that is processed electronically (eg by computer); is recorded manually (eg on paper) with the intention of being processed electronically (eg collected on paper and then scanned onto computer); is recorded as part of a relevant filing system (see below);
Data controller	is the organisation that determines the purposes for which and the manner in which personal data are processed. Discover Kings Lynn is the data controller. Employees, managers, contractors and other staff are not data controllers;
Data processor	is an external organisation that we appoint to process personal data on our behalf. Examples of these might include
Data Protection Officer	Amanda Davies
Data subject	is a living, identifiable individual about whom we process personal data;
Information Commissioner	is the supervisory authority responsible for enforcing the provisions of the Act in England and Wales;
Personal data	are data which relate to a living individual who can be identified from those data or from those data and other information which is in our possession or likely to come into our possession. Personal data include opinions and indications of our intentions towards an individual;
Processing	has a wide meaning and covers virtually anything that can be done in relation to personal data, such as obtaining, recording, holding, altering, retrieving, consulting, using, disclosing, blocking, erasing or destroying personal data;
Relevant filing system	is a set of manual information (ie paper files) relating to individuals which is structured by reference to individuals or criteria relating to them in such a way that specific information relating to a particular individual is readily accessible;
Sensitive personal data	means information as to (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) his trade union membership, (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, and (h) any

proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

THE PRINCIPLES

First principle
Personal data must be processed fairly and lawfully and must not be processed unless (a) at least one of the conditions in Schedule 2 is met and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

This is the first and possibly most important of all the principles. It requires us to process personal data fairly and lawfully. Each of these requirements is considered in turn below.

Lawful processing

The Act prohibits the processing of any personal data unless that processing can be justified under one of a number of conditions which are set out in Schedules 2 and 3 of the Act. It is worth remembering the very broad definition of 'processing' which includes obtaining, disclosing, using and viewing.

You must justify your processing of **all** personal data under one of the conditions set out in Schedule 2. If you cannot find a condition that justifies your processing then that processing may **not** take place. The most relevant Schedule 2 conditions are:

1 The data subject has given his consent to the processing.

2 The processing is necessary in order to enter into or perform a contract with the data subject.

3 The processing is necessary for compliance with any legal obligation to which King's Lynn BID Limited is subject (other than an obligation imposed by contract).

4 The processing is necessary in order to protect the vital interests of the data subject.

5 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment,

6 The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

When considering the above conditions remember the broad definition of processing. For example, obtaining consent to the processing of personal data means obtaining consent to the disclosure, collection, use, destruction etc of personal data.

In addition, where you are processing sensitive personal data, you must also justify that processing under one of the conditions in Schedule 3. This is a safeguard which recognises the sensitive and sometimes confidential nature of this category of personal data. The most relevant Schedule 3 conditions are:

7 The data subject has given his explicit consent to the processing.

8 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on King's Lynn BID Limited in connection with employment.

9 The processing is necessary (a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

10 The processing (a) is necessary for the purposes of, or in connection with, any actual or prospective legal proceedings, (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

11 The processing is necessary for the (a) administration of justice, (b) exercise of any functions conferred on any person by or under any enactment, or (c) exercise of any functions of the Crown, a Minister of the Crown or a government department

12 The processing is necessary for medical purposes and is undertaken by (a) a health professional or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

13 The processing (a) is of sensitive personal data consisting of information as to racial or ethnic origin, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

14 The processing (a) is in the substantial public interest, (b) is necessary for the purposes of the prevention or detection of any unlawful act, and (c) must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes.

15 The processing (a) is of sensitive personal data consisting of information as to religious beliefs or other beliefs of a similar nature; or physical or mental health or condition, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons holding different religious beliefs; or different states of physical or mental health or conditions, with a view to enabling such equality to be promoted or maintained, and (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject; and (d) does not cause,

nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

16 The processing (a) is in the substantial public interest, (b) is necessary for research purposes, (c) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of that data subject, and (d) does not cause, nor is likely to cause, substantial damage or distress to the data subject or any other person.

Remember: unless you can justify your processing of sensitive personal data under both Schedules 2 and 3, you may **not** process those data.

Fair processing

The second requirement of the first principle is that personal data must be processed fairly. In broad terms what this means is that we must ensure transparency of processing so that data subjects are aware of who is processing their personal data and why. We achieve this by giving data subjects a data protection notice which meets the following requirements:

Content of data protection notice:

- the identity of the data controller King's Lynn BID Limited
- the purposes for the processing (if one of those purposes is marketing then we should include a description of the communication channels that we intend to use and offer the data subject an opportunity to object. If any of those channels involve marketing by email, SMS, fax or automated calling systems, we need (as a general rule) to obtain the data subject's consent)
- any other information that is necessary to make the processing fair (such as any recipients of the data and their purposes, a reminder of the data subject's right of access and correction, whether any of the information we are asking for is mandatory or voluntary and whether there will be any transfers of personal data to countries outside the European Economic Area (which comprises the EU Member States plus Iceland, Norway and Liechtenstein).

Timing of data protection notice:

- The data protection notice must be given to the data subject at the right time. Where we obtain personal data directly from the data subject (eg as a result of a telephone call, or online collection) we must give the notice to the data subject at the time we obtain his data
- Where we obtain personal data about a data subject from a third-party source (eg a family member or a list rental provider) we must provide the data protection notice as soon as reasonably practicable after we have started processing his data (unless it would be a disproportionate effort to do so)

Position and format of data protection notice:

- The data protection notice must be reasonably prominent and in reasonably legible font

- The data protection notice must be included at every point where we collect personal data, such as application forms and website activity
- If, for example, the data protection notice is provided online, it must be positioned so that it can be seen and not hidden behind a hypertext link and should be included in the online journey just before a 'submit' button

You can obtain copies of our standard and current data protection notices from the Data Protection Officer. These notices have been drafted to take account of the kind of processing that we do. You should use the data protection notices whenever you obtain personal data. You must not modify any of these notices without prior authority. These notices have been drafted so that they comply with the Act and any modification on your part could change that. If you think the notices do not cover your particular processing activities you must discuss this in the first instance with the Data Protection Officer

Second principle
Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with those purposes.

The second data protection principle sets out two requirements:

- personal data must be obtained only for one or more specified and lawful purposes. Our data protection notices will specify the purposes for which we will process personal data and we are not permitted to process those data for a new purpose (unless the data subject gives his consent).
- personal data must not be further processed in any manner incompatible with the purpose or purposes for which the data were obtained. A breach of this principle could also result in a breach of the first principle. For example, if a data protection notice describes the purposes for which personal data will be used as administration, marketing and risk assessment, we should not use those data for any other purposes, unless those additional purposes would be totally obvious to the individual. To do otherwise could result in unfair processing in breach of the first principle and a breach of the second principle.

Third principle
Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

The third data protection principle requires that personal data must be adequate, relevant and not excessive. You must, therefore, ensure:

- you identify the personal data needed for a particular purpose and you collect the minimum amount required to properly fulfil that purpose
- you do not hold personal data on a 'just-in-case' basis because you think it might be useful in the future but without having any clear idea of what that future purpose might be

- you keep personal data up to date (otherwise personal data which were originally adequate may cease to be so)
- you do not keep personal data for too long (otherwise those data may cease to be relevant and become excessive).

Fourth principle
Personal data must be accurate and, where necessary, kept up to date.

Personal data will be inaccurate if they are incorrect or misleading as to any matter of fact (eg an incorrect name or address). If you are inputting data onto our system and are unsure as to the accuracy of certain information (eg because you cannot read the handwriting or because it looks like an obvious mistake or omission), you should try to get in touch with the data subject to clarify the issue.

We will not be in breach of this principle, even if we are holding inaccurate personal data if:

- we accurately recorded those data when we received them from the data subject or a third party and
- we took reasonable steps to ensure the accuracy of those personal data and
- if the data subject has notified us that the personal data are inaccurate, we have taken steps to indicate this fact (eg by making a note that we have received an objection).

You must take reasonable steps to keep personal data up to date to the extent necessary. The purpose for which personal data are held will determine whether they need to be kept up to date or not. For example, historical records of transactions should not, as a general rule, be updated.

Fifth principle
Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.

You should review the personal data which you hold on a regular basis and delete any data which are no longer required in connection with the purpose for which they were originally obtained. When carrying out this exercise you should consider any legal or other requirements to retain data. You should also consider the type of relationship which King's Lynn BID Limited has with the data subject and whether there is an expectation that we will retain data for any given period of time (eg our employees would expect us to retain their data for a period of time after they had left so we could provide them with a reference, or in the event of an employment claim).

Sixth principle
Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

The rights which are referred to in the sixth principle are the data subject's rights in relation to:

- access to his personal data
- preventing processing likely to cause damage or distress
- preventing processing for the purposes of direct marketing
- automatic decision-taking

If you receive a request in writing from an individual mentioning any of the above rights, you must pass that request promptly to the Data Protection Officer as there are strict timescales within which we must respond.

Seventh principle
Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The seventh principle requires King's Lynn BID Limited to take appropriate technical and organisational measures to protect personal data which we process:

- technical measures include: software controls to restrict user access; up-to-date virus checking software; audit trail software; and encryption all of which we have in place and manage through our
- organisational measures include: restricting access to buildings and computer rooms; ensuring secure disposal of information; and training staff on the care and handling of personal data all of which you are responsible for complying with and applying to your daily routine.

The Act imposes upon King's Lynn BID Limited additional obligations if we use third parties to process personal data on our behalf. Examples of these third parties might include our external payroll providers, the company that provides disaster recovery services, the company that hosts our website. Some of these third parties may have access to, or need to process, personal data on our behalf. If so, they will be acting as our data processors and the Act requires us to:

- put in place a contract in writing with each of our data processors under which they agree to act only on instructions from us;
- include the right to audit our data processors to ascertain compliance with the data protection requirements of the data processing contract; and
- ensure that the data processor agrees to comply with obligations equivalent to those imposed on us by the seventh principle.

If you are responsible for the selection, appointment or use of data processors, you must ensure that you only select those processors that are able to provide us with sufficient guarantees in respect of the

technical and organisational measures they will apply to the processing of personal data. Furthermore, if you are responsible for the drafting or negotiation of contracts with data processors, you must ensure those contracts contain all applicable data protection provisions. Seek further advice from the Data Protection Officer

Eighth principle
Personal data must not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

You must not transfer any personal data to any country or territory outside the European Economic Area (**EEA**), unless you are authorised to do so. The EEA comprises the EU Member States plus Iceland, Norway and Liechtenstein. Be aware that transfers may take place that are not obvious—e.g. if a data processor that we have appointed in the UK subcontracts some of its processing obligations to a sub-processor in India there will be a transfer of data out of the EEA (from the data processor to the sub-processor) which will be prohibited unless certain conditions are met.

If you need to transfer personal data to a country or territory outside the EEA you must consult with the Data Protection Officer who will advise you further on how to comply with the adequacy requirements of the eighth principle.

DATA SUBJECT RIGHTS

The sixth data protection principle requires us to comply with the rights of data subjects. It is important for you to familiarise yourself with these rights so that you may be able to identify them more easily. Each one is described below.

Right of subject access

Data subjects have a right of access to their personal data. A request for access will usually include a request for specific or general information relating to the applicant. If we receive such a request we must provide a description of:

- the personal data relating to that data subject
- the purposes for which the data are being processed
- the recipients of the data
- the information constituting the personal data
- the source of those data (if available).

The Act lays down timescales within which we must comply with a request and requirements regarding how the information must be supplied. If you are authorised to handle subject access requests, you should follow the rules and procedures set out in the Subject Access Request Policy. If you are not authorised to handle such requests, you should not attempt to do so, but should forward the request to the Data Protection Officer

Right to prevent processing likely to cause damage or distress

Data subjects have the right to ask us not to process their personal data if:

- the processing of those data in a particular way or for a particular purpose is causing, or is likely to cause, substantial damage or substantial distress to that data subject or another person; and
- that damage or distress is, or would be, unwarranted.

You can usually identify a request to exercise this right because it will ask us to stop processing personal information about the individual. The Act lays down timescales within which we must comply with such a request. If you receive a request to stop processing you must forward it promptly to the Data Protection Officer You should not attempt to deal with a request on your own.

Right to prevent processing for the purposes of direct marketing

Data subjects have the right to request that we stop processing their personal data for direct marketing purposes. This means we must stop sending direct marketing materials to anyone that objects. You can identify a request made under this right because it is likely to ask us to stop sending unwanted marketing materials, otherwise referred to as 'junk mail' or 'spam', or stop making marketing calls.

If you receive a request to exercise this right you should forward it promptly to the **Data Protection Officer** who will take the appropriate action to ensure that the individual's details are suppressed on our marketing database and he or she is no longer contacted by us for marketing purposes.

Right to object to automated decision taking

Data subjects have the right to object to automated decisions being taken about them in relation to important matters that significantly affect them (such as evaluating performance at work, creditworthiness, reliability or conduct). This right is complex and subject to certain conditions. You can identify a request made under this right because it is likely to mention automated decisions or decisions made by computer and may ask us to take that decision again manually (ie using an individual instead of a computer).

If you receive a request from any person exercising their right to object to automated decisions being taken about them, you should forward that request promptly to the Data Protection Officer. You should not try to handle the request yourself.

Additional data subject rights

In addition to the rights specifically referred to in the sixth principle, data subjects also have the following rights:

- the right to ask the Information Commissioner to carry out an assessment as to whether or not King's Lynn BID Limited's processing is in accordance with the Act. This means the data subject has the right to make a complaint to the Commissioner and ask him to investigate. The Commissioner is obliged to consider all such requests and this could result in an investigation of our processing activities;
- the right to take legal action against King's Lynn BID Limited in the courts and claim compensation for any damage (or damage and distress) the data subject has suffered as a result of a breach of the Act ; and
- the right to apply to court for an order to rectify, block, erase or destroy inaccurate personal data and any expression of opinion based on those inaccurate data.

Consequences of non-compliance

If we are found to be in breach of the Act, the Information Commissioner may impose a monetary penalty of up to £500,000 (depending on the seriousness of the breach). The Commissioner could also issue enforcement proceedings against us which could result in our being prevented from further use of the affected personal data, or being required to change our processing procedures, or having other conditions imposed upon us in respect of the processing of personal data. Enforcement action will usually have a cost and time implication for the business. However, more damaging might be any restrictions imposed upon us which prevent us from exploiting our databases commercially. Additionally, the associated publicity could make us appear as an organisation that does not respect the privacy rights of individuals.

Affected data subjects may also take legal action against us and claim compensation for any breaches of the Act on our part that have resulted in damage (or damage and distress) to the data subject.

In certain circumstances, a negligent or deliberate breach of the Act could result in criminal liability not just for King's Lynn BID Limited but also for our employees and other members of staff. For these reasons it is essential to comply with the provisions of the Data Protection Policy and this Guidance.

Contacts and responsibilities

If you have any queries regarding the Data Protection Policy, this Guidance or compliance with the Act in general, please contact the Data Protection Officer for further advice.

The Data Protection Policy and this Guidance will be updated from time to time by the Data Protection Officer to reflect any changes in legislation or in our methods or practices.

October 2017