**DATA PROTECTION & PRIVACY POLICY**

**The Data Protection Act in Practice**

Green Light Sites Ltd needs to keep certain information about its employees. It is also necessary to process information so that GLS can comply with its legal obligations and staff can be recruited and paid. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this, Green Light Sites must comply with the Data Protection Principles which are set out in the Data Protection Act 2018 (the 2018 Act) and the General Data Protection Regulation (UK GDPR) and the [Privacy and Electronic Communications Regulations](http://www.legislation.gov.uk/uksi/2003/2426) PECR.

The Data Protection Act applies to ‘personal data’ (GLS may also use the term ‘Confidential’ data in some of its policies). That is, data about identifiable living individuals that can be used to identify them. It may also consist of two or more non identifiable pieces of information that used together can identify a specific living individual.

Those who decide how and why personal data are processed (data controllers), must comply with the rules of good information handling, known as data protection principles, and the other requirements of the Data Protection Act 2018 (UK GDPR). It is the policy of Green Light Sites Ltd to comply with the rules and requirements of the Act. To meet this obligation we will conform to the following:

**What is Personal Data?**

Personal data: any information relating to a living individual who can be directly or indirectly identified from it.

This includes:-

* Name, Address, contact details
* Maybe two or more non-specific pieces of information that when combined identify an individual
	+ gender, birth date, geographic indicator and other descriptors.

Special categories of personal data:

* racial or ethnic origin,
* Political opinions,
* religious or philosophical beliefs,
* trade union membership,
* genetic & biometric information, health & a natural person’s sex life or sexual orientation.

**The rules of good information handling – the principles**

Anyone processing personal data in the organisation will comply with the eight enforceable principles of good practice. Furthermore, The organization is responsible for, and must be able to demonstrate compliance with, the GDPR's principles:

Data must be:-

“(a) processed lawfully, fairly and in a transparent manner in relation to individuals (‘**lawfulness, fairness and transparency**’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘**purpose limitation’**);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation’**);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(‘accuracy’**);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals **(‘storage limitation’**);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality’**).”

**The Data Controller**

Green Light Sites Ltd as a corporation is the Data Controller under the 2018 Act.

Any member of staff, applicant or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself should raise the matter with the appropriate Designated Data Controller.

Green Light Sites also work as Data Processors on behalf of our charity clients. In doing so Green Light Sites shall act in accordance with the act 2018 in all matters of Data Processing. GLS shall hold a valid enforceable contract with the client who will be the data controller.

**Responsibilities of Staff**

All staff are responsible for:

* Checking that any information that they provide to Green Light Sites Ltd in connection with their employment is accurate and up to date.
* Informing Green Light Sites Ltd of any changes to information that they have provided, e.g. changes of address, either at the time of appointment or subsequently. GLS cannot be held responsible for any errors unless the staff member has informed them of such changes.

**Consent**

Consent must be a freely given, specific, informed, and unambiguous indication of the individual's wishes. Consent may be withdrawn at any time.

**Green Light Sites Ltd.’s Data Protection Code of Practice**

**Data Security**

1. All staff are responsible for ensuring that:
* Any personal data that they hold is kept securely.
* Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.
1. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
2. Personal information should:
* Be kept in a locked filing cabinet, drawer, or safe; or
* If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
* If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

**Collection and Amendment of Personal Data**

1. **Collection of personal data**: In most cases, the personal data held by Green Light Sites Ltd will be obtained directly from the data subjects themselves. The law stipulates that a data protection notice must accompany any request for personal data.
2. **Security of personal data**: Of fundamental importance within any data protection regime is the security of the personal data that is being processed. Data subjects have the right to expect that their personal data will be kept and processed securely and that no unauthorised disclosures or transfers will take place to anyone either within or outside of Green Light Sites Ltd. Authorised disclosures or transfers are those that are defined within the appropriate Notifications and declared to the data subject either at the point of data collection or subsequently, the necessary consent for disclosure or transfer having been obtained if required.
3. To help ensure the security of personal data within Green Light Sites Ltd, all staff who process such data in the course of performing their duties are required to follow the general guidelines set out below.
4. **Secure storage of personal data**: Each member of staff whose work involves storing personal data, whether in electronic or paper format, must take personal responsibility for its secure storage, in line with Green Light Sites Ltd.’s Data Protection Policy, which states that personal data should:
* Be kept in a locked filing cabinet, drawer, or safe; or
* If it is computerised, be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up; and
* If a copy is kept on a diskette or other removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
1. Unless agreed with a line manager or senior manager, personal data should never be stored at staff members’ homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.
2. **Secure processing of personal data**: While staff members in the course of performing their legitimate duties are using personal data, reasonable precautions must be taken to ensure the safety and privacy of that data. For example:
* In open-plan offices, computer screens that could potentially be displaying personal data should not be positioned such that unauthorised staff may readily see that data, and password protected screensavers should be used.
* Personal data in manual form, such as in paper files, correspondence or database printouts, should not be left in view in open-plan offices while the relevant staff members are away from their desks. They should instead be locked away or at least covered.
* Where manual records containing personal data are accessible to a number of staff in the course of their legitimate activities, access logbooks should be used where practicable to help monitor the whereabouts and use of such records.

**The disclosure and transfer of personal data**

1. **Authorised and unauthorised disclosures:** Staff members working with personal data will be made aware by their line managers or other appropriate staff of the purposes for which the data is processed and the legitimate parties either within or outside Green Light Sites Ltd. to whom that data, either in whole or in part, may be disclosed or transferred. Personal information must not be disclosed either orally or in writing or via Web pages or by any other means, manual or electronic, accidentally or otherwise, to any unauthorised third party.
2. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.
3. **Security of data during transfer**: Where personal data is transferred between staff members within Green Light Sites or between authorised suppliers or charity clients in the course of their legitimate activities, the level of security appropriate to the type of data and anticipated risks should be applied. For example, sensitive personal data should either be transferred by internal mail in sealed envelopes or by hand. If transferred by e-mail, such data should be encrypted. If documents are password protected the password must be supplied via a separate channel. Personal data must never be transferred by instant messaging or text message (SMS).

**Retention and Disposal of Personal Data**

1. **The retention of personal data:** Green Light Sites Ltd. has a duty to retain some staff personal data for a period of time following their departure from the company, mainly for legal reasons, but also for other purposes such as being able to provide references or for financial reasons, for example relating to pensions and taxation.
2. The disposal of personal data: When a record containing personal data is to be disposed of, the following procedures will be followed:
* All paper documentation containing personal data will be permanently destroyed by shredding or incinerating, depending on the sensitivity of the personal data.
* All computer equipment or media that are to be sold or scrapped will have had all personal data completely destroyed, by re-formatting, over-writing or degaussing.

**Notification of Data Breach**

1. Should you become aware of any personal data being breached you must report to (Information Security Committee) Liam McEntegart or Lewis Honney immediately.
2. The ISC shall conduct a Data breach self assessment.
3. Data breaches of Personal Data should be assessed and reported to the ICO within 72 hours.

**Guidance notes**

Personal data covers both facts and opinions about an individual. It also includes information regarding the intentions of the data controller towards the individual.

‘Processing’ is broadly defined and takes place when any operation or set of operations is carried out on personal data. The Act requires that personal data be processed “fairly and lawfully”. Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject must be told the identity of the data controller and why that information is to be processed.

*Processing may only be carried out where one of the following conditions has been met:*

1. The individual has given his or her consent to the processing;

2. The processing is necessary for the performance of a contract with the individual;

3. The processing is required under legal obligation;

4. The processing is necessary to protect the vital interests of the individual;

5. The processing is necessary to carry out public functions;

6. The processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could prejudice the interests of the individual).

**Processing sensitive data**

The Data Protection Act makes specific provision for sensitive personal data. Sensitive data includes: racial or ethnic; political opinions; religious or other beliefs; trade union membership; health; sexual orientation; criminal proceedings or convictions.

*Sensitive data can only be processed under strict conditions, which include:*

1. having the explicit consent of the individual;

2. being required by law to process the data for employment purposes;

3. needing to process the information in order to protect the vital interests of the data subject or another;

4. dealing with the administration of justice or legal proceedings.

**Paper files**

The Data Protection Act covers information which is recorded as part of a 'relevant filing system', that is, a set of information in which the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that 'specific information relating to a particular individual is readily accessible'. The definition means a significant amount of manual data falls under the scope of the Data Protection Act, as does the extension of the definition of data to cover 'accessible records'.

**Security**

Data controllers must take security measures to safeguard personal data. The 2018 Act requires that data controllers must take appropriate technical or organisational measures to prevent the unauthorised or unlawful processing, or disclosure, of data. Where a controller uses the services of a data processor the security arrangements must be part of a written agreement between the two.

**Notification**

Most data controllers will need to notify the Data Protection Register, in broad terms, of the purposes of their processing, the personal data processed, the recipients of the personal data processed and the places overseas to which the data are transferred. This information is made publicly available in a register. Notification is not linked to enforcement. Under the 2018 Act all data controllers must comply with the data protection principles, even if they are exempt from the requirement to notify. Data controllers have a single register entry. Notifications are renewable annually.

**The rights of individuals**

*The right to be informed*

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. We must provide individuals with information including: the purpose for processing their personal data, the retention periods for that personal data, and who it will be shared with.

*The right of access*

The Data Protection Act allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of access. Individuals have the right to access and receive a copy of their personal data, and other supplementary information.

*The right of rectification*

The UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing..

*The right to restrict processing*

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the personal data, but not use it.

*Rights in relation to automated decision-taking including profiling.*

An individual can ask a data controller to ensure that no decision, which significantly affects them, is based solely on processing his or her personal data by automatic means. There are, however, some exemptions to this.

*Right to erasure:*

Individuals have the right to have their personal data erased, also known as the 'right to be forgotten,' if the data is no longer necessary for the purpose it was collected, or if they withdraw their consent. The right is not absolute and only applies in certain circumstances. Individuals can make a request for erasure verbally or in writing.

*Right to Data Portability:*

The UK GDPR grants individuals the right to data portability, allowing them to obtain and reuse their personal data across different services by transferring it from one IT environment to another safely and securely.

*Right to Object:*

Individuals have the right to object to the processing of their personal data under UK GDPR, particularly for direct marketing, research, or statistical purposes, and the processing must stop immediately upon request.

**Telecommunications**

PECR are the [Privacy and Electronic Communications Regulations](http://www.legislation.gov.uk/uksi/2003/2426). Their full title is The Privacy and Electronic Communications (EC Directive) Regulations 2003. They are derived from European law. They implement [European Directive 2002/58/EC](http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058), also known as ‘the e-privacy Directive’. The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications. Our practices remain in line with the Privacy and Electronic Communications Regulations (PECR) as amended by the UK's exit from the EU.

There are specific rules on:

* marketing calls, emails, texts and faxes;
* cookies (and similar technologies);
* keeping communications services secure; and
* customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

Direct marketing is defined in section 122(5) of the Data Protection Act 2018 (UK GDPR) as:

“the communication (by whatever means) of advertising or marketing material which is directed to particular individuals”. This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds. The marketing must be directed to particular individuals.

The rules on live marketing calls are in regulation 21, 21A and 21B. In short, you must not make unsolicited live calls:

* to anyone who has told you they don’t want your calls;
* to any number registered with the TPS or CTPS, unless the person has specifically consented to your calls – even if they are an existing customer (unless the call is in relation to pension schemes and you meet a strict criteria, see below);

You must always say who is calling, allow your number (or an alternative contact number) to be displayed to the person receiving the call, and provide a contact address or freephone number if asked.

The TPS is the Telephone Preference Service. It is a central register of individuals who have opted out of receiving live marketing calls.

The CTPS is the Corporate TPS. It works in the same way as the TPS, but for companies and other corporate bodies (limited liability partnerships, Scottish partnerships and government bodies).

For more information and details of how to subscribe to the TPS/CTPS, see [www.tpsonline.org.uk](http://www.tpsonline.org.uk/tps/index.html).

You can call any individual who has specifically consented to receive marketing calls from you – for example, by ticking an opt-in box. See [What counts as consent?](https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/#consent)

You can also make live calls without consent to a number if it is not listed on the TPS – but only if that person hasn’t objected to your calls in the past and you are not marketing claims management services.

In practice, this means you will need to screen most call lists against the TPS register. You will also need to keep your own ‘do not call’ list of people who object or opt out, and screen against that as well.

**Criminal Offences**

*Notification offences*

These are committed where processing is being undertaken by a data controller who has not notified the Register either of the processing being undertaken or of any changes that have been made to that processing. Failure to notify is a strict liability offence.

*Procuring and selling offences*

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also an offence to access personal data or to disclose it without proper authorisation. This covers unauthorised access to and disclosure of personal data. There are some exceptions to this.

*Enforced subject access offence*

Unless one of the limited statutory exceptions applies, it is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person for specified purposes, such as a precondition to employment.

*Other offences*

It is an offence to fail to respond to an information notice or to breach an enforcement notice.

*Correcting Incorrect Data*

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible at the above address. We will promptly correct any information found to be incorrect.

*For further guidance on our data protection obligations, refer to the Information Commissioner’s Office (ICO) guidance.*[*http://www.ico.gov.uk/*](http://www.ico.gov.uk/)