DATA PROTECTION POLICY

Introduction

The purpose of this document is to provide a concise policy regarding the data protection obligations of **Sunseeker Windows**.

Sunseeker Windows is a data controller with reference to the personal data which it manages, processes and stores.

Scope

The policy covers both personal and sensitive personal data held in relation to its data subjects by **Sunseeker Windows**. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by **Sunseeker Windows**. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

Definitions

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy.

Data	This includes both automated and manual data. • Automated data means data held on computer, or stored with the intention that it is processed on computer. • Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
Personal Data	Information that relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of **Sunseeker Windows**.
Sensitive Personal Data	Sensitive personal data is personal data which relates to specific aspects of one's identity or personality, and includes information relating to ethnic or racial identity, political or ideological beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record.
Data Controller	The legal entity responsible for the acquisition, processing and use of the personal data. In the context of this policy; **Sunseeker Windows** is the data controller.
Data Subject	A living individual who is the subject of the personal data, i.e. to whom the data relates either directly or indirectly.
Data Processor	A person or entity who processes personal data on behalf of **Sunseeker Windows** on the basis of a formal, written contract, but who is not an employee of **Sunseeker Windows**.
Data Protection Officer	A person appointed by **Sunseeker Windows** to monitor compliance with the appropriate data protection legislation, to deal with Subject Access Requests, and to respond to data protection queries from staff members and the general public.

SUNSEEKER WINDOWS AS A DATA CONTROLLER

In the course of its daily organisational activities, **Sunseeker Windows** acquires, processes and stores personal data in relation to living individuals. To that extent, **Sunseeker Windows** is a data controller, and has obligations under the Data Protection legislation, which are reflected in this document.

In accordance with GDPR, this data must be acquired and managed fairly.

Sunseeker Windows is committed to ensuring that all staff members have sufficient awareness of the legislation in order to be able to anticipate and identify a data protection issue, should one arise. In such circumstances, staff members must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by **Sunseeker Windows**, there is a regular and active exchange of personal data between **Sunseeker Windows** and its data subjects. In addition, **Sunseeker Windows** exchanges personal data with data processors on the data subjects' behalf. This is consistent with **Sunseeker Windows's** obligations under the terms of its contracts with its data processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the DPO to seek clarification.

Third-Party Processors (where applicable)
In the course of its role as data controller, **Sunseeker Windows** engages third-party service providers, or data processors, to process personal data on its behalf.

In each case, a formal, written contract is in place with the processor, outlining their obligations in relation to the personal data, the security measures that they must have in place to protect the data, the specific purpose or purposes for which they are engaged, and the understanding that they will only process the data in compliance with GDPR.

The Data Protection Rules
The following key rules are enshrined in GDPR and are fundamental to **Sunseeker Windows's** data protection policy.

In its capacity as data controller, **Sunseeker Windows** ensures that all data shall:

1. Be obtained and processed fairly and lawfully

For data to be obtained fairly, the data subject will, at the time the data are being collected, be made aware of:

- The identity of the data controller (**Sunseeker Windows**);
- The purpose(s) for which the data is being collected;
- The person(s) to whom the data may be disclosed by the data controller;
- Any other information that is necessary so that the processing may be fair.

Sunseeker Windows will meet this obligation in the following way:

- Where possible, the informed consent of the data subject will be sought before their data is processed;

- Where it is not possible to seek consent, **Sunseeker Windows** will ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;

- Where **Sunseeker Windows** intends to record activity on CCTV or video, a Fair Processing Notice will be posted in full view, prior to the recording;

- Processing of the personal data will be carried out only as part of **Sunseeker Windows's** lawful activities, and it will safeguard the rights and freedoms of the data subject;

- The data subject's data will not be disclosed to a third party other than to a party contracted to **Sunseeker Windows** and operating on its behalf, or where **Sunseeker Windows** is required to do so by law.

2. Be obtained only for one or more specified, legitimate purposes

Sunseeker Windows will obtain data for purposes which are specific, lawful and clearly stated. A data subject will have the right to question the purpose(s) for which **Sunseeker Windows** holds their data, and it will be able to clearly state that purpose or purposes.

3. Not be further processed in a manner incompatible with the specified purpose(s)

Any use of the data by **Sunseeker Windows** will be compatible with the purposes for which the data was acquired.

4. Be kept safe and secure

Sunseeker Windows will employ high standards of security in order to protect the personal data under its care. **Sunseeker Windows's** Password Policy and Data Retention and Destruction Policies guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by **Sunseeker Windows** in its capacity as data controller.

Access to, and management of, staff and customer records is limited to those staff members who have appropriate authorisation and password access.

In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third-party processor will notify the data controller without undue delay.

5. Be kept accurate, complete and up to date where necessary

Sunseeker Windows will:

- Ensure that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;

- Conduct periodic reviews and audits to ensure that relevant data is kept accurate and up to date. **Sunseeker Windows** conducts a review of sample data every six months to ensure accuracy;

- Conduct regular assessments in order to validate the need to keep certain personal data.

6. Be adequate, relevant and not excessive in relation to the purpose(s) for which the data were collected and processed

Sunseeker Windows will ensure that the data it processes in relation to data subjects are relevant to the purposes for which those data are collected. Data which are not relevant to such processing will not be acquired or maintained.

7. Not be kept for longer than is necessary to satisfy the specified purpose(s)

Sunseeker Windows has identified an extensive matrix of data categories, with reference to the appropriate data retention period for each category. The matrix applies to data in both a manual and automated format.

Once the respective retention period has elapsed, **Sunseeker Windows** undertakes to destroy, erase or otherwise put this data beyond use.

8. Be managed and stored in such a manner that, in the event a data subject submits a valid Subject Access Request seeking a copy of their personal data, this data can be readily retrieved and provided to them

Sunseeker Windows has implemented a Subject Access Request procedure by which to manage such requests in an efficient and timely manner, within the timelines stipulated in the legislation.

Data Subject Access Requests

As part of the day-to-day operation of the organisation, **Sunseeker Windows's** staff engages in active and regular exchanges of information with data subjects. Where a valid, formal request is submitted by a data subject in relation to the personal data held by **Sunseeker Windows** which relates to them, such a request gives rise to access rights in favour of the Data Subject.

There are specific time-lines within which **Sunseeker Windows** must respond to the data subject, depending on the nature and extent of the request. These are outlined in the attached Subject Access Request process document.

Sunseeker Windows's staff will ensure that such requests are forwarded to the Data Protection Officer in a timely manner, and they are processed as quickly and efficiently as possible, but within not more than one month from receipt of the request.

DATA SECURITY POLICY

Sunseeker Windows Personal Data Security Policy

Procedures and Guidelines
Sunseeker Windows is committed to ensuring the protection of the privacy of the personal and sensitive personal data which it controls, and in order to assist in the **Sunseeker Windows's** compliance with the data protection legislation will provide best practice guidelines and procedures in relation to all aspects of data security and protection.

Privacy and Confidentiality Protocol.
Sunseeker Windows staff are aware of the Data Subjects' right to the utmost privacy and confidentiality in the processing of their personal data. To ensure that our Data Subjects' privacy is respected and delivered to the utmost standard, all staff working in **Sunseeker Windows** are bound by a "**Confidentiality Agreement"** within the terms of their employment**.**

Security and Computer Usage Policy
Sunseeker Windows provides a variety of electronic communications systems for use in carrying out its business. All communication and information transmitted by, received from or stored in these systems are the property of **Sunseeker Windows** and, as such, are intended to be used for job-related purposes only.

The following summary guidelines regarding access to and disclosure of data on any **Sunseeker Windows** electronic communication systems will help to better determine how to use these systems in light of **Sunseeker Windows**'**s** privacy and security policy.

Monitoring
Sunseeker Windows [in conjunction with third-party service provider(s)] provides the network, personal computers, electronic mail, tough books and mobile phones for staff use while conducting company business. **Sunseeker Windows** may access, monitor and disclose all data or messages stored on its systems or sent over its electronic mail system.

The company also reserves the right to disclose the contents of such messages for any purpose at its sole discretion. No monitoring or disclosure will occur without the direction of either IT Management, or executive leadership, or as required by law, unless otherwise noted.

Passwords
Initial passwords are assigned by the IT department and will not be given to other staff or persons outside the organization. Employees will be prompted to change the provided passwords as soon as possible using the instructions provided by the IT staff. These passwords may be changed from time to time

Legal Proceedings
Information sent by employees via the electronic mail system may be considered legal documents, and may be used in legal proceedings.

Physical Security
Access to computer rooms will be limited to staff who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive will be secured in a locked room or office during non-business hours.

Equipment which is to be removed from **Sunseeker Windows** property must be approved in advance with the IT department and an inventory of this equipment maintained by IT.

Where the employee leaves the organization, he or she must return the equipment to **Sunseeker Windows** prior to the last day of employment.

Network Security

IT will monitor network security on a regular basis. Adequate information concerning network traffic and activity will be logged to ensure that breaches in network security can be detected. IT will also implement and maintain procedures to provide adequate protection from intrusion into **Sunseeker Windows** computer systems from external sources. No computer that is connected to the network can have stored, on its disk(s) or in its memory, information that would permit access to other parts of the network. Staff should not store personal, business, member or other credit card/account information, or passwords within word processing or other data documents.

Personal Computer Security

Only legally licensed software and Virus Protection will be installed on **Sunseeker Windows** computers. Software cannot be removed, copied or installed without the permission or involvement of the IT department.

All staff will log out of the network and turn their computers off before leaving the office at the end of each working day.

Staff will lock their screens by using "CNTRL+ALT+DLT" keys when leaving their desk and computer unattended for a short period of time.

Staff will log off from the network when they will be away from their desk for an extended period.

Failure to comply with all components of this Data Security Policy may result in disciplinary action up to and including termination of employment.

Virtual Private Network

A Virtual Private Network (VPN) is established to enable staff working on the system from outside the organisation's offices to access data via an encrypted "tunnel" to protect information moving on a network.

Restricted Access

Access to servers is restricted to the systems administrator [and the middleware administrator]. This access is needed to maintain the function of middleware and to troubleshoot processing problems. These information technology experts are aware of the highly sensitive nature of the person's personal data contained in the system and their responsibilities in terms of privacy and confidentiality and have signed a confidentiality agreement as part of their contract of employment.

All third-party service providers will agree and sign a Data Processor Contract with **Sunseeker Windows** prior to the commencement of their engagement. The terms of this contract will be negotiated between **Sunseeker Windows** and the Service Provider, and will reflect both parties' obligations under the GDPR regulation.

Business Continuity Management

Sunseeker Windows and its third party Service Providers will employ appropriate business continuity measures to ensure the efficient recovery of full operational functionality in a timely manner, in the event of a catastrophic or destructive event which renders normal system access impossible.

CCTV

Introduction

Closed Circuit Television Systems (CCTV) are installed on the premises under the control of **Sunseeker Windows**.

Scope

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The policy applies equally to personal data obtained by **Sunseeker Windows** via CCTV which is subsequently held in manual and automated form.

Justification for the use of CCTV

The General Data Protection Regulation (GDPR) requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that **Sunseeker Windows** needs to be able to justify the obtaining and use of personal data by means of a CCTV system.

Location of Cameras

The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. **Sunseeker Windows** endeavors to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed to record external areas are positioned in such a way as to prevent, or minimize, recording of passers-by or of another person's private property.

CCTV Video Monitoring and Recording of Public Areas under the remit of **Sunseeker Windows** may include the following:

- Protection of buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas.
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms.
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control.
- Criminal Investigations (carried out by an appropriate authority): Robbery, burglary and theft surveillance.

Siting Cameras

Each CCTV camera should be sited in such a way that it monitors those spaces/areas which are intended to be covered. Where this cannot be avoided, the system software has been utilised to "blank out" spaces/areas where monitoring should not occur.

Operators must be aware that they may only use the cameras solely for the purposes for which they were installed.

Operators must also be aware of the position a camera is left in after use. A camera when not in use should be placed in the most advantageous position to record incidents occurring within its field of vision.

Training
Appropriate training in the requirements of the General Data Protection Regulation (GDPR) will be given to all staff. Staff that are required to manage and work the CCTV Systems will be fully trained in respect of all functions, both operational and administrative relating to the control of the CCTV Systems.

Camera Signage
Signs have been placed so that persons are aware that they are entering an area which is covered by **Sunseeker Windows's** CCTV System. They are clearly visible and legible to members of the public.

Retention of Images
The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the DPO.

When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis. Images must not be retained for longer than is necessary. Images will be erased after a period of 28 days unless required for the investigation of offences or evidential purposes.

The Data Controller shall ensure that copies of recorded images will only be made under the following circumstances:

- The incident recorded is such that it is required to assist in the investigation of offences and/or the prosecution of offenders;
- For training purposes within that context and with due regard to personal privacy;
- At the request of an appropriate authority in the course of the investigation of a suspected crime;
- Where a copy is required to satisfy a valid Subject Access Request.

Access to and Disclosure of Images to Third Parties
Access to images will be restricted to staff that need to have access in order to achieve the purposes of using the equipment. All access to the medium on which the images are recorded will be documented by the Designated Manager.

The disclosure of recorded images to Third Parties must be authorised by **Sunseeker Windows**.

- A request for disclosure of images, from a member of an appropriate authority, on the grounds that the images are likely to be of use for the investigation of a particular offence or an investigation into an accident or similar incident;
- A requirement under any enactment, rule of law or court order to disclose the images;
- If required by a legal representative of **Sunseeker Windows**;
- If a case/action is being taken against **Sunseeker Windows**;
- To people whose images have been recorded or retained, in satisfaction of a valid Subject Access Request (unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings).

WEBSITE PRIVACY POLICY

The policy: This privacy policy is for this website; [sunseekerwindows.co.uk] and served by [Sunseeker Windows Ltd, 72-84 Station Road, Burton Latimer, NN15 5NX] and governs the privacy of its users who choose to use it. It explains how we comply with the GDPR (General Data Protection Regulation), the DPA (Data Protection Act) [pre GDPR enforcement] and the PECR (Privacy and Electronic Communications Regulations).

We are firmly committed to protecting and respecting your personal information and privacy. As such, your personal details will never be released to any outside company for mailing or marketing purposes. This notice sets out how data will be used and you should therefore carefully consider this document. By providing us with data you are consenting to the practices set out in this notice.

You may withdraw your consent to processing of information at any time. If you wish to do so then please contact (insert name) on (insert number). If you are unhappy with how your data has been processed then please contact us in the first instance or the ICO.

Information We May Collect

Details of prospective employees

Details of customers and prospective customers

Details of third parties that may assist us from time to time

This may include but is not limited to names, addresses, next of kin, date of birth, national insurance number, driving license details, banking details etc. It may be shared with third parties such as HMRC etc. We will hold no more information that is absolutely necessary to achieve our objective in relation to you.

How We Use Your Information

We will only use your information for a lawful purpose such providing a service. We will use the information for the specific purpose in question and will use the minimum data necessary to achieve this. We will always ensure that any information is accurate and up to date.

If you are a prospective employee we will use the information to assess your suitability for any roles we may have. The information will be destroyed after a reasonable time if your application is unsuccessful.

If you are a customer we will use your information for any enquiry and will destroy the information after a reasonable time unless you are an ongoing repeat customer.

We may disclose any information to a third party such as a government department as required by law.

If your information is added to a mailing list then we will require your consent in relation to the same.

If you are a child then we will require the consent of an adult to hold information about you.

Storage of Data

All of the information you provide us will be held on secure servers. It may from time to time be transferred to a third party as and when required for processing. Unfortunately, the internet is never

100% secure so we can only use our best endeavors to ensure that your information is not accessed unlawfully. If we establish that there has been a breach of security then we will take appropriate action.

Use of Cookies

This website uses cookies to better the users experience while visiting the website. As required by legislation, where applicable this website uses a cookie control system, allowing the user to give explicit permission or to deny the use of /saving of cookies on their computer / device.

What are cookies?

Cookies are small files saved to the user's computer's hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server to provide the users with a tailored experience within this website. Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors or use the cookie control system if available upon their first visit.

Website Visitor Tracking

This website uses tracking software to monitor its visitors to better understand how they use it. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information.

Adverts and Sponsored Links

This website may contain sponsored links and adverts. These will typically be served through our advertising partners, to whom may have detailed privacy policies relating directly to the adverts they serve.

Clicking on any such adverts will send you to the advertiser's website through a referral program which may use cookies and will track the number of referrals sent from this website. This may include the use of cookies which may in turn be saved on your computer's hard drive. Users should therefore note they click on sponsored external links at their own risk and we cannot be held liable for any damages or implications caused by visiting any external links mentioned.

Downloads and Media Files

Any downloadable documents, files or media made available on this website are provided to users at their own risk. While all precautions have been undertaken to ensure only genuine downloads are available users are advised to verify their authenticity using third party anti-virus software or similar applications.

We accept no responsibility for third party downloads and downloads provided by external third party websites and advise users to verify their authenticity using third party anti-virus software or similar applications.

Contact and Communication with us

Users contacting us through this website do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use.

Where we have clearly stated and made you aware of the fact, and where you have given your express permission, we may use your details to send you products/services information through a mailing list system. This is done in accordance with the relevant regulations named in 'The policy' above.

Email Mailing List and Marketing Messages

We may operate an email mailing list program, used to inform subscribers about products, services and/or news we supply/publish. Users can subscribe through an online automated process where they have given their explicit permission. Subscriber personal details are collected, processed, managed and stored in accordance with the regulations named in 'The policy' above. Subscribers can unsubscribe at any time through an automated online service.

External Website Links and Third Parties

Although we only look to include quality, safe and relevant external links, users are advised to adopt a policy of caution before clicking any external web links mentioned throughout this website.

Social Media Policy and Usage

We adopt a Social Media Policy to ensure our business and our staff conduct themselves accordingly online. While we may have official profiles on social media platforms users are advised to verify authenticity of such profiles before engaging with, or sharing information with such profiles. We will never ask for user passwords or personal details on social media platforms. Users are advised to conduct themselves appropriately when engaging with us on social media.

There may be instances where our website features social sharing buttons, which help share web content directly from web pages to the respective social media platforms. You use social sharing buttons at your own discretion.

DATA SUBJECT ACCESS REQUEST

Sunseeker Windows Subject Access Request (SAR) Policy

Sunseeker Windows is aware of its obligations as a Data Controller, with primary responsibility for, and a duty of care towards the personal data within its control.

Data Subjects whose personal data is held by **Sunseeker Windows** are entitled to ask Data Controllers:

• Whether the Data Controller is processing any personal data about that individual and, if so, to be given:-

- a description of the personal data;
- the purposes for which they are being processed; and
- information on any organisation to whom that personal data is being, or might be disclosed.
- to be told about the sources from which the Data Controller derived the information so long as those sources are available to the Controller; and
- For a copy of the information held, in response to a valid request to that effect.

Form of the request
A request for Personal Data is a known as a Subject Access Request. However, it may not always be necessary to treat a request for information as a formal request under the General Data Protection Regulation (GDPR)

If the request for information is one which **Sunseeker Windows** would normally deal with within the normal course of business, e.g. a request for a copy of a statement by a bank customer, **Sunseeker Windows** will consider whether this is a formal subject access request under the DP Acts, or whether it can be managed as a 'business-as-usual' process.

In order to be valid, a Subject Access Request should be in writing, and should include sufficient information to identify the Data Subject to the Data Controller's satisfaction.

When these criteria are satisfied, the Subject Access Request is considered valid, and the 1-month response period commences.

Sunseeker Windows will strive to respond to a valid request as quickly as possible, but nonetheless within this 1-month period.

Communicating with the Data Subject
Sunseeker Windows will communicate directly with the Data Subject once a valid Subject Access
Request has been received.

Rather than having to provide a copy of all data held by the Controller, this contact may help the Data Subject to specify the exact information he or she wishes to receive, thereby reducing both effort and the time and cost required to collate and provide the data being sought.

However, we acknowledge that, where the Data Subject is adamant that he or she wishes to receive a copy of everything the Data Controller holds about them, then we will fulfil a complete and exhaustive search of the computerised and manually-held data in the organisation.

Systems Search
Unless there is a legitimate option to reduce the scope of the Request, a search of all databases and all relevant filing systems (manual files) which are relevant under the Acts will be carried out throughout the organisation.

There is no obligation to search back-up files, on the basis that the data in back-up is a copy of the data already held either on the 'active' systems, or in archive.

Sunseeker Windows will organise the response to the Request by giving one individual the responsibility for issuing requests for information throughout the organisation and receiving all the returns. This coordinator role will normally fall to the Data Protection Officer, where one has been appointed.

The coordinator will then have the job of printing out all computerised information which has been returned to them by each department. They will also have received photocopies of all relevant manual files, and will therefore collate two sets of material – one of computer printouts and the other of photocopied manual files.

Manual files
The manual files which are relevant to the Acts are those which pass the conditions set out in the definition of a relevant filing system. The key criterion is whether the file in question forms part of a structured set. The set has to be structured by reference to the Requestor or characteristics relating to Requestor. If, for example, the manual files are organised in alphabetical name order, or by payroll number, they will form a structured set.

Restrictions following receipt of a request
Compliance with the DP Acts is not intended to interfere with the normal running of a Data Controller's business and following the receipt of a valid Request, we are permitted to make changes to the requested information in the normal course of operation provided that no changes are made because of the Request itself; this applies even where the Data Controller would rather not release the information in its current form. This includes the correction of any incorrect data held as the principle is that the individual has a right to request the actual information held about them (whether or not it is accurate or correct).

Third party data
Once the information has been collected, the Request coordinator will consider their obligations to other data subjects.

The coordinator will put themselves 'in the shoes' of the individual making the Subject Access Request. They have to read every single page of information to see whether it reveals the identity of any third party, when viewed from the perspective of the person making the Request. If the identity of a third party is already known to the Data Subject, then the data containing the information relating to the third party can be revealed to the Data Subject, because he/she is already aware of that information.

However, where the identity of a third party is not already known to the Data Subject in the context revealed by the documents, then the Request coordinator will consider whether the Request requires the disclosure of the information relating to the third party or whether it is possible to separate this information from the other information to be disclosed, for example, by blanking out (redacting) the name of the individual, or blanking out other identifying particulars or any other material, would be sufficient to disguise the identity of the third party from the Data Subject.

At this point, all other information which is likely to come into the hands of the Data Subject must be considered as well. If the identifying material can be blanked out with black marker pen and the rest

of the information on that page can be handed over without revealing the identity of the third party, then this information will be included in fulfilling the Subject Access Request.

Exemptions
Some material is exempt from inclusion in the response to a Subject Access Request.

This includes the content of negotiations with the Data Subject. If the Data Controller is negotiating with the Data Subject at the time at which the Data Subject makes the Subject Access Request, the Data Controller does not have to reveal requested information if to do so would be likely to prejudice those negotiations. Once the negotiations are complete and have been put into effect, the whole file becomes subject to Subject Access in the normal way.

Emails are subject to Subject Access, as are archived computerised and manual data. It must be remembered that CCTV footage and tapes of telephone conversations will also be included within the scope of the Request, and must be searched on receipt of a Subject Access Request if the data subject so requires.

Other general exemptions to subject access are national security and the prevention or detection of crime, or the apprehension or prosecution of offenders.

Where the personal data contain health information, there is a duty on the Data Controller to consult an appropriate health professional before the information can be released to the Data Subject. This is to avoid disclosing information about adverse health conditions to a Data Subject where the disclosure may be harmful or distressing to the Data Subject or to another person.

This requirement does not apply where the Data Subject has already had access to the information, or where the Data Subject originally provided the information himself or herself.

We recognise that failure to respond to a Subject Access Request within the 1 month period gives rise to the ability of the individual to complain to the Information Commissioners Office (ICO), and may well give rise to an investigation by the Commissioner and will breach legislation.

It is possible to do so, **Sunseeker Windows** will liaise with the Data Subject as to the form in which we hand over the information to the Data Subject.

The default position is that the Data Subject gets a hard copy of the information in a “permanent and intelligible format” (which may make it necessary for any internal codes released with the information to be explained), unless the supply of such a copy is not possible or would involve a disproportionate effort, or the Data Subject agrees otherwise. Any terms which are not intelligible without an explanation must be accompanied by an explanation (e.g. a Glossary of Terms).

Finally, once the response to the Subject Access Request has been finalised, the Request coordinator will make a full copy of the material to be retained for our own reference.

The copy of the requested material will be dispatched by secure, registered delivery, and we will seek timely confirmation from the Data Subject on receipt of the material.

These records will be used as reference material should, in the future, there is any dispute as to the content or timeliness of the response provided to the Data Subject.

DATA RETENTION POLICY

1. Introduction

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);

b) When the data subject withdraws their consent;

c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;

d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);

e) When the personal data has to be erased to comply with a legal obligation; or

f) Where the personal data is processed for the provision of information society services to a child.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Company complies fully with its obligations and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by the Company, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

This Policy applies to all personal data held **Sunseeker Windows** and by third-party data processors processing personal data on the Company's behalf, whether it be on computer, laptop, mobile device, phone or physical document.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully informed of their rights, of what personal data the Company holds about them, how that personal data is used and how long the Company will hold that personal

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of the right to restrict the Company's use of their personal data and further rights relating to automated decision-making and profiling

5. Technical and Organisational Data Security Measures

5.1 The following technical measures are in place within the Company to protect the security of personal data. Please refer to the Company's Personal Data Security Policy for further details:

a) All emails containing personal data must be encrypted;

b) All emails containing personal data must be marked "confidential";

c) Personal data may only be transmitted over secure networks;

d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;

f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;

g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent securely by post etc.

h) All personal data transferred physically should be transferred in a suitable container marked "confidential";

i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from DPO.

j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;

k) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;

l) Personal data must be handled with care at all times and should not be left unattended or on view;

m) Computers used to view personal data must always be locked before being left unattended;

n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;

o) All personal data stored electronically should be backed up All backups should be encrypted;

p) All electronic copies of personal data should be stored securely using passwords and encryption these must never be shared.

q) All passwords used to protect personal data should be changed regularly and must be secure;

r) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;

s) No software may be installed on any Company-owned computer or device without approval; and

t) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of DPO to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data.

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, securely destroyed, or otherwise disposed of.

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;

b) The type of personal data in question;

c) The purpose(s) for which the data in question is collected, held, and processed;

d) The Company's legal basis for collecting, holding, and processing that data;

e) The category or categories of data subject to whom the data relates;

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).

7.6 In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Ref.	**Type of Data**	**Purpose of Data**	**Review Period**	**Retention Period or Criteria**	**Comments**
<<insert ref>>	<<insert data type>>	<<describe purpose of data>>	<<insert review date or period>>	<<insert retention period>>	<<add additional information as required>>

DATA DESTRUCTION POLICY

Overview

Personal data in manual (paper-based) format, and the technology equipment on which such data is stored in electronic (automated) format, cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and required by law.

Paper files, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of data, some of which is considered both commercially and personally sensitive. In order to protect the data, all storage mediums must be properly disposed of. Electronic media should also be 'wiped' prior to being appropriately destroyed, to remove any risk that confidential or sensitive data remains retrievable.

However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

Sunseeker Windows is aware of its obligations to retain personal data in a safe and secure manner for as long as necessary, and to then dispose of such data in an appropriate manner.

This Data Destruction Policy outlines the Company's approach to fulfilling such obligations, and is closely aligned with the Company's Data Retention Policy.

Purpose

This policy has been developed to define the requirements for proper disposal of manual and electronic data at **Sunseeker Windows**.

Scope

This policy applies to all personal data held by **Sunseeker Windows** in both manual and electronic formats.

Policy

Manual Data Disposal

1. **Sunseeker Windows** will schedule a regular review of its retention of manual records, and will schedule timely destruction of paper-based records where retention has exceeded [the Company's] operational requirements and Regulatory obligations.
2. These manual records will be collected and stored in a secure environment, prior to destruction;
3. **Sunseeker Windows** will make paper cross-cut shredders available within the organisation in order to dispose of paper records which have no, or short-term retention periods – this may include (but are not limited to) general office correspondence, hand-written notes used prior to transcription, copies of documents which might have been used for short-term cross-reference, etc.
4. Within the terms of **Sunseeker Windows's** Retention Policy, staff will be trained and aware of their obligation to shred such material using these in-house shredders.
5. For the bulk disposal of paper records for which there is a medium- to long-term retention obligation, **Sunseeker Windows** will appoint an appropriately specialised third party to process

the act of destruction of these records, using approved and recognised industry standard methods;

6. The third party will be required to sign an appropriate Data Processor contract, as per requirements from the appropriate legislation;

Technology Equipment Disposal

7. **Sunseeker Windows** will schedule a regular collection of end of life technology equipment, throughout the organisation. This equipment will be collected and stored in a secure environment, prior to destruction;
8. Technology equipment included in the scope of this policy are:
    a. Internal Hard Drives (Physical/SSD);
    b. External hard Drives (Physical/SSD);
    c. RAM Modules;
    d. Tapes (DAT/DLT/LTO);
    e. CD/DVD/Blu-ray;
    f. Mobile Phones/PDAs;
    g. USB Sticks;
9. **Sunseeker Windows** will appoint an appropriate third party to process the act of destruction of this equipment, using approved and recognised industry standard methods;
10. The third party will be required to sign an appropriate Data Processor contract, as per requirements from the appropriate legislation;

DATA LOSS NOTIFICATION PROCEDURE

Introduction
Sunseeker Windows is aware of its obligations as a data controller, with primary responsibility for, and a duty of care towards the personal data within its control.

Rationale
The response to any breach of personal data (as defined by the legislation) can have a serious impact on **Sunseeker Windows**'s standing within the national and international community.

The consequential impact of a data breach on a commercial brand can often be immeasurable therefore; exceptional care must be taken when responding to data breach incidents.

As such, not all data protection incidents result in data breaches, and not all data breaches require notification. This guide is therefore designed to assist staff in developing an appropriate response to a data breach, based on the specific characteristics of the incident.

Scope
This policy document covers both personal data and sensitive personal data held by **Sunseeker Windows**. The policy applies equally to personal data held in manual and automated form.

All personal data and sensitive personal data will be treated with equal care by **Sunseeker Windows**. Both categories will be equally referred-to as personal data within this policy, unless specifically stated otherwise.

What constitutes a breach?
A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to personal data in usable form, whether manual or automated.

This could mean:

- Loss of a laptop, memory stick or mobile device that contains personal data;
- Lack of a secure password on PCs and applications;
- Emailing a list of employee-related information to someone in error;
- Giving a system login to an unauthorised person;
- Failure of a door lock or some other weakness in physical security which compromises personal data.

What happens if a breach occurs?

Actual, suspected, or potential breaches should be reported immediately to **Sunseeker Windows**'s Data Protection Officer (DPO)

Any staff member who becomes aware of a likely data breach and fails to notify the DPO will be subject to **Sunseeker Windows**'s disciplinary procedure.

A team comprising of the DPO, and other relevant staff members will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of data subjects impacted, the Information Commissioners Office (ICO) and relevant regulatory bodies will be informed as quickly as possible following detection, but in any event an initial report will be made within 24 hours of first becoming aware of the breach.

In certain circumstances **Sunseeker Windows** may (e.g. if required by the Information Commissioners Office (ICO)), inform the data subjects of the loss of their data and provide them with an assessment of the risk to their privacy. **Sunseeker Windows** will make recommendations to the data subjects which may minimise the risks to them. **Sunseeker Windows** will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

In appropriate cases, following a data breach **Sunseeker Windows** may notify organisations that may be required for, and are capable of, assisting in the protection of data subjects' personal data; for example, an appropriate legal authority, the HSE, relevant financial institutions etc.

When will the Office of the Information Commissioners Office (ICO) be informed?

All incidents in which personal data has been put at risk will be reported to the Information Commissioners Office (ICO). The only exceptions to this policy are when the data subjects have already been informed, where the loss affects fewer than 100 data subjects, where the device on which the data was stored was fully encrypted, and where the loss involves only non-sensitive, non-financial personal data.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Information Commissioners Office (ICO) is notified only where the data on such devices is not encrypted.

Should the Office of the Information Commissioners Office (ICO) request **Sunseeker Windows** to provide a detailed written report of the incident, the Commissioner will specify a time-frame for the delivery of the report which will be appropriate to the nature of the data breach and the quantity of information that is required.

Depending on the size and seriousness of a data breach, the Information Commissioners Office (ICO) may conduct an investigation into the circumstances surrounding the breach. Investigations may include an on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident if **Sunseeker Windows** has not already done so. Where necessary, the Office of the Data Protection Commissioner may use its enforcement powers to demand appropriate action from **Sunseeker Windows** in order to protect the interests and rights of data subjects.

Data Loss Incident logging

All data breaches will be recorded in an incident log as required by the Information Commissioners Office (ICO). The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request.

SUMMARY

1. **Roles and Responsibilities**

1.1 The Company's Data Protection Officer is **insert details**

1.2 The Data Protection Officer shall be responsible for overseeing the implementation of and compliance with this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

1.3 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

2. **Implementation of Policy**

This Policy shall be deemed effective as of 25th May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Jeremy Cattell

Position Managing Director

Date: 25.05.2018

Due for Review by: 25.05.2021

Signature: