DATA PROTECTION AND DATA SECURITY POLICY

Statement and Purpose of Policy

A. SUNK RECORDINGS LTD (the **Employer**) is committed to ensuring that all personal data handled by us will be processed according to legally compliant standards of data protection and data security.

B. We confirm for the purposes of the data protection laws, that the Employer is a data controller of the personal data in connection with your employment. This means that we determine the purposes for which, and the manner in which, your personal data is processed.

C. The purpose of this Policy is to help us achieve our data protection and data security aims by:

1. notifying our staff of the types of personal information that we may hold about them, our customers, suppliers and other third parties and what we do with that information;
2. setting out the rules on data protection and the legal conditions that must be satisfied when we collect, receive, handle, process, transfer and store personal data and ensuring staff understand our rules and the legal standards; and
3. clarifying the responsibilities and duties of staff in respect of data protection and data security.

D. This is a statement of policy only and does not form part of your contract of employment. We may amend this Policy at any time, in our absolute discretion.

E. For the purposes of this Policy:

1. **Data protection laws** means all applicable laws relating to the processing of personal data, including, for the period during which it is in force, the UK General Data Protection Regulation.
2. **Data subject** means the individual to whom the personal data relates.
3. **Personal data** means any information that relates to an individual who can be identified from that information.
4. **Processing** means any use that is made of data, including collecting, storing, amending, disclosing, or destroying it.
5. **Special categories of personal data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

Data Protection Principles

1. Staff whose work involves using personal data relating to Staff or others must comply with this Policy and with the following data protection principles which require that personal information is:

a. **processed lawfully, fairly and in a transparent manner.** We must always have a lawful basis to process personal data, as set out in the data protection laws. Personal data may be processed as necessary to perform a contract with the data subject, to comply with a legal obligation which the data controller is the subject of, or for the legitimate interest of the data controller or the party to whom the data is disclosed. The data subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed.

b. **collected only for specified, explicit and legitimate purposes.** Personal data must not be collected for one purpose and then used for another. If we want to change the way we use personal data, we must first tell the data subject.

c. **processed only where it is adequate, relevant and limited to what is necessary for the purposes of processing.** We will only collect personal data to the extent required for the specific purpose notified to the data subject.

d. **accurate and the Employer takes all reasonable steps to ensure that information that is inaccurate is rectified or deleted without delay.** Checks to personal data will be made when collected and regular checks must be made afterwards. We will make reasonable efforts to rectify or erase inaccurate information.

e. **kept only for the period necessary for processing.** Information will not be kept longer than it is needed and we will take all reasonable steps to delete information when we no longer need it. For guidance on how long particular

information should be kept, contact the Data Protection Officer.

f. **secure, and appropriate measures are adopted by the Employer to ensure as such.**

Who is Responsible for Data Protection and Data Security?

2. Maintaining appropriate standards of data protection and data security is a collective task shared between us and you. This Policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, casual or agency staff, trainees, homeworkers and fixed-term staff and any volunteers (**Staff**).

3. Questions about this Policy, or requests for further information, should be directed to the Data Protection Officer.

4. All Staff have personal responsibility to ensure compliance with this Policy, to handle all personal data consistently with the principles set out here and to ensure that measures are taken to protect the data security. Managers have special responsibility for leading by example and monitoring and enforcing compliance. The Data Protection Officer must be notified if this Policy has not been followed, or if it is suspected this Policy has not been followed, as soon as reasonably practicable.

5. Any breach of this Policy will be taken seriously and may result in disciplinary action up to and including dismissal. Significant or deliberate breaches, such as accessing Staff or customer personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

What Personal Data and Activities are Covered by This Policy?

6. This Policy covers personal data:

   a. which relates to a natural living individual who can be identified either from that information in isolation or by reading it together with other information we possess;

   b. is stored electronically or on paper in a filing system;

   c. in the form of statements of opinion as well as facts;

   d. which relates to Staff (present, past or future) or to any other individual whose personal data we handle or control;

   e. which we obtain, is provided to us, which we hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

7. This personal data is subject to the legal safeguards set out in the data protection laws.

What Personal Data Do We Process About Staff?

8. We collect personal data about you which:

   a. you provide or we gather before or during your employment or engagement with us;

   b. is provided by third parties, such as references or information from suppliers or another party that we do business with; or

   c. is in the public domain.

9. The types of personal data that we may collect, store and use about you include records relating to your:

   a. home address, contact details and contact details for your next of kin;

   b. recruitment (including your application form or curriculum vitae, references received and details of your qualifications);

   c. pay records, national insurance number and details of taxes and any employment benefits such as pension and health insurance (including details of any claims made);

   d. telephone, email, internet, fax or instant messenger use;

   e. performance and any disciplinary matters, grievances, complaints or concerns in which you are involved.

Sensitive Personal Data

10. We may from time to time need to process sensitive personal information (sometimes referred to as 'special categories of personal data').
11. We will only process sensitive personal information if:
    a. we have a lawful basis for doing so, e.g. it is necessary for the performance of the employment contract; and
    b. one of the following special conditions for processing personal information applies:
        i. the data subject has given explicit consent.
        ii. the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject.
        iii. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent.
        iv. processing relates to personal data which are manifestly made public by the data subject.
        v. the processing is necessary for the establishment, exercise, or defence or legal claims; or
        vi. the processing is necessary for reasons of substantial public interest.
12. Before processing any sensitive personal information, Staff must notify the Data Protection Officer of the proposed processing, in order for the Data Protection Officer to assess whether the processing complies with the criteria noted above.
13. Sensitive personal information will not be processed until the assessment above has taken place and the individual has been properly informed of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
14. Our Privacy Notice sets out the type of sensitive personal information that we process, what it is used for and the lawful basis for the processing.

How We Use Your Personal Data

15. We will tell you the reasons for processing your personal data, how we use such information and the legal basis for processing in our Privacy Notice. We will not process Staff personal information for any other reason.
16. In general, we will use information to carry out our business, to administer your employment or engagement and to deal with any problems or concerns you may have, including, but not limited to:
    a. **Staff address lists:** to compile and circulate lists of home addresses and contact details, to contact you outside working hours.
    b. **Sickness records:** to maintain a record of your sickness absence and copies of any doctor's notes or other documents supplied to us in connection with your health, to inform your colleagues and others that you are absent through sickness, as reasonably necessary to manage your absence, to deal with unacceptably high or suspicious sickness absence, to inform reviewers for appraisal purposes of your sickness absence level, to publish internally aggregated, anonymous details of sickness absence levels.
    c. **Monitoring IT systems:** to monitor your use of e-mails, internet, telephone and fax, computer or other communications or IT resources.
    d. **Disciplinary, grievance or legal matters:** in connection with any disciplinary, grievance, legal, regulatory or compliance matters or proceedings that may involve you.
    e. **Performance reviews:** to carry out performance reviews.

Accuracy and Relevance

17. We will:
    a. ensure that any personal data processed is up to date, accurate, adequate, relevant and not excessive, given the purpose for which it was collected.

b. not process personal data obtained for one purpose for any other purpose, unless you agree to this or reasonably expect this.

18. If you consider that any information held about you is inaccurate or out of date, then you should tell the Data Protection Officer. If they agree that the information is inaccurate or out of date, then they will correct it promptly. If they do not agree with the correction, then they will note your comments.

Storage and Retention

19. Personal data (and sensitive personal information) will be kept securely in accordance with our Information Security Policy.

20. The periods for which we hold personal data are contained in our Privacy Notices.

Individual Rights

21. You have the following rights in relation to your personal data.

22. Subject access requests:

    a. You have the right to make a subject access request. If you make a subject access request, we will tell you:

        i. whether or not your personal data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;

        ii. to whom your personal data is or may be disclosed, including to recipients outside of the UK or European Economic Area (EEA) and the safeguards that apply to such transfers;

        iii. for how long your personal data is stored (or how that period is decided);

        iv. your rights of rectification or erasure of data, or to restrict or object to processing;

        v. your right to right to complain to the Information Commissioner if you think we have failed to comply with your data protection rights; and

        vi. whether or not we carry out automated decision-making and the logic involved in any such decision making.

    b. We will provide you with a copy of the personal data undergoing processing. This will normally be in electronic form if you have made a request electronically, unless you agree otherwise.

    c. To make a subject access request, contact us at dee@sunkrecordings.co.uk.

    d. We may need to ask for proof of identification before your request can be processed. We will let you know if we need to verify your identity and the documents we require.

    e. We will normally respond to your request within 28 days from the date your request is received. In some cases, eg where there is a large amount of personal data being processed, we may respond within 3 months of the date your request is received. We will write to you within 28 days of receiving your original request if this is the case.

    f. If your request is manifestly unfounded or excessive, we are not obliged to comply with it.

23. Other rights:

    a. You have a number of other rights in relation to your personal data. You can require us to:

        i. rectify inaccurate data;

        ii. stop processing or erase data that is no longer necessary for the purposes of processing;

        iii. stop processing or erase data if your interests override our legitimate grounds for processing the data (where we rely on our legitimate interests as a reason for processing data);

        iv. stop processing data for a period if data is inaccurate or if there is a dispute about whether or not your interests override the Employer's legitimate grounds for processing the data.

    b. To request that we take any of these steps, please send the request to dee@sunkrecordings.co.uk.

Data Security

24. We will use appropriate technical and organisational measures to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

25. Maintaining data security means making sure that:

    a. only people who are authorised to use the information can access it;

    b. where possible, personal data is pseudonymised or encrypted;

    c. information is accurate and suitable for the purpose for which it is processed; and

    d. authorised persons can access information if they need it for authorised purposes.

26. By law, we must use procedures and technology to secure personal information throughout the period that we hold or control it, from obtaining to destroying the information.

27. Personal information must not be transferred to any person to process (eg while performing services for us on or our behalf), unless that person has either agreed to comply with our data security procedures or we are satisfied that other adequate measures exist.

28. Security procedures include:

    a. Any desk or cupboard containing confidential information must be kept locked.

    b. Computers should be locked with a strong password that is changed regularly or shut down when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others.

    c. Data stored on CDs or memory sticks must be encrypted or password-protected and locked away securely when they are not being used.

    d. The Data Protection Officer must approve of any cloud used to store data.

    e. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.

    f. All servers containing sensitive personal data must be approved and protected by security software.

    g. Servers containing personal data must be kept in a secure location, away from general office space.

    h. Data should be regularly backed up in line with the Employer's back-up procedure.

29. Telephone precautions. Particular care must be taken by Staff who deal with telephone enquiries to avoid inappropriate disclosures. In particular:

    a. the identity of any telephone caller must be verified before any personal information is disclosed;

    b. if the caller's identity cannot be verified satisfactorily then they should be asked to put their query in writing;

    c. do not allow callers to bully you into disclosing information. In case of any problems or uncertainty, contact the Data Protection Officer.

30. Methods of disposal. Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

Data Impact Assessments

31. Some of the processing that the Employer carries out may result in risks to privacy.

32. Where processing would result in a high risk to Staff rights and freedoms, the Employer will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

Data Breaches

33. If we discover that there has been a breach of Staff personal data that poses a risk to the rights and freedoms of individuals, we will report it to the Information Commissioner within 72 hours of discovery.

34. We will record all data breaches regardless of their effect in accordance with our Breach Response Policy.

35. If the breach is likely to result in a high risk to your rights and freedoms, we will tell affected individuals that there has been a breach and provide them with more information about its likely consequences and the mitigation measures it has taken.

International Data Transfers

36. In the course of carrying out our business, we may need to transfer your personal information to a country outside the UK or European Economic Area (EEA) including to any group company or to another person with whom we have a business relationship.
37. Your personal data will only be transferred to a country outside of the UK or EEA if there are adequate protections in place. To ensure that your personal data receives an adequate level of protection, we have put in place appropriate procedures with the third parties we share your personal data with, to ensure your personal data is treated by those third parties in a way that is consistent with and which respects the law on data protection.
38. If you wish to know more about international transfers of your personal data, you may contact the Data Protection Officer.

Individual Responsibilities

39. Staff are responsible for helping the Employer keep their personal data up to date.
40. Staff should let the Employer know if personal data provided to the Employer changes, e.g. if you move house or change your bank details.
41. You may have access to the personal data of other Staff members and of our customers in the course of your employment. Where this is the case, the Employer relies on Staff members to help meet its data protection obligations to Staff and to customers.
42. Individuals who have access to personal data are required:
    a. to access only personal data that they have authority to access and only for authorised purposes;
    b. not to disclose personal data except to individuals (whether inside or outside of the Employer) who have appropriate authorisation;
    c. to keep personal data secure (e.g. by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
    d. not to remove personal data, or devices containing or that can be used to access personal data, from the Employer's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
    e. not to store personal data on local drives or on personal devices that are used for work purposes.

Training

43. We will provide training to all individuals about their data protection responsibilities as part of the induction process and at regular intervals thereafter.
44. Individuals whose roles require regular access to personal data, or who are responsible for implementing this Policy or responding to subject access requests under this Policy will receive additional training to help them understand their duties and how to comply with them.

Attribution

45. This Data Protection and Data Security Policy was created using a document from Rocket Lawyer (https://www.rocketlawyer.com/gb/en).

DATA RETENTION POLICY AND SCHEDULE

Statement of Purpose

1. SUNK RECORDINGS LTD (the **Organisation**, **we**, **our** or **us**) is committed to adhering to the data protection and privacy rights of all individuals whose Personal Data it Processes in the course of its activities. To do so, we are committed to meeting the requirements imposed by UK Data Protection Laws: particularly, requirements under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This Data Retention Policy is implemented to this end, with a focus on the storage limitation principle.
2. This Data Retention Policy is based on the UK Data Protection Laws. If this Policy is at any time inconsistent with this body of law, SUNK RECORDINGS LTD will act (including by adjusting any relevant Retention Periods) to meet the requirements imposed by up-to-date UK Data Protection Laws in priority to the requirements set out in this Policy.
3. Any questions in relation to this Policy should be referred to the Data Protection Officer in the first instance, via email at dee@sunkrecordings.co.uk.

Definitions, Interpretation, and Scope

4. Within this Policy, the following terms hold the following meanings:
    a. '**Condition for Processing**' means the exceptions to the general prohibition on Processing Special Category Personal Data, specified by UK Data Protection Laws, at least one of which must apply to Processing of Special Category Personal Data for that Processing to be in compliance with UK Data Protection Laws;
    b. '**Data Protection Principles**' means the 7 core principles at the heart of the UK Data Protection Laws, which these laws are constructed to uphold;
    c. '**Data Subject**' means the individual to whom an item of Personal Data relates and who can be identified from this data;
    d. '**Lawful Bases**' means the 6 grounds set out in Article 6 of the UK GDPR, at least one of which must apply to Processing of Personal Data for that Processing to be in compliance with UK Data Protection Laws;
    e. '**Personal Data**' means any information relating to an individual who can be identified (either directly or indirectly) by this information. References to Personal Data within this Policy refer to all Personal Data that the Organisation Processes, including any Personal Data that the Organisation stores following use of this data in the course of its work with or via agents, consultants, sub-contractors, or similar;
    f. '**Processing**' means any use of Personal Data outside of private personal use, including obtaining, recording, managing, using, storing, or anonymising this data;
    g. '**Special Category Personal Data**' means the certain types of personal data that the UK Data Protection Laws identify as being more sensitive in nature than other Personal Data and, consequently, as requiring a higher level of protection; including information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, and biometric data;
    h. '**UK Data Protection Laws**' means any law applicable in the UK relating to the Processing of Personal Data, including but not limited to the UK GDPR and the Data Protection Act 2018.
5. The definitions above apply also to the singular or plural, other tense, or other form of such words when used within this Policy.

Legal Justification for Processing

6. SUNK RECORDINGS LTD is committed to ensuring that all Processing of Personal Data carried out by us and/or our agents, sub-contractors, consultants, employees, or others working on our behalf is carried out in compliance with UK Data Protection Laws. As such, we confirm that:
    a. All Personal Data is Processed in reliance on one or more of the Lawful Bases;

b. All Special Category Personal Data is, additionally, Processed in reliance on a separate Condition for Processing; and

c. All Processing is carried out in accordance with the Data Protection Principles.

7. All necessary documentation and procedures are completed and in place to ensure that all Processing is carried out in accordance with UK Data Protection Laws and the Data Protection Principles (e.g. the transparency and accountability principles).

a. Access to documentation can be requested from the Data Protection Officer by emailing dee@sunkrecordings.co.uk. Access will be granted where it is appropriate to do so (e.g. with regard to other individuals' data privacy and to business confidentiality needs).

Storage Limitation

8. This Data Retention Policy deals primarily with how we will uphold the Data Protection Principle of storage limitation. The storage limitation principle requires that we do not keep (e.g. store) Personal Data for any longer than we need it, with 'need' determined by reference to the purposes and Lawful Bases for which given Personal Data is Processed.

9. Adhering to the storage limitation principle is vital for:

a. Reducing the risks of data breaches and other security threats to data's privacy and integrity;

b. Reducing the risk of Personal Data becoming irrelevant, excessive, inaccurate, out-of-date; or being used incorrectly or by accident; and

c. Reducing the Organisation's legal risk by ensuring that Personal Data is not retained once the applicable Lawful Bases(s) no longer apply (i.e. once it can no longer be Processed in accordance with UK Data Protection Laws).

10. To uphold the storage limitation principle, SUNK RECORDINGS LTD's commitments include (but are not limited to):

a. Adhering to the Retention Periods set out in the schedule to this Policy titled 'Schedule - Retention Periods';

b. No longer storing Personal Data that, despite not yet having been held for the duration of the applicable Retention Period, is inappropriate to store with regard to UK Data Protection Laws and other laws (e.g. when there is no requirement that it is retained longer for purposes such as maintaining compliant tax and employment records or dealing with legal claims);

c. Properly handling any individuals' data erasure requests and, where appropriate, complying with such requests; and

d. Deleting or anonymising Personal Data that is no longer needed in accordance with this Policy.

Retention Periods

11. A **Retention Period** is a set time period after which the applicable type of Personal Data should be considered no longer needed and should be deleted or anonymised, unless a situation applies that requires certain Personal Data to be stored for longer and which justifies its further Processing (including storing) under UK Data Protection Laws. Justifications and decisions on extended storage periods can be identified and proposed by the Staff Member responsible for the applicable Personal Data, then should be approved by the Data Protection Officer before being implemented.

12. Once Personal Data has reached the end of its Retention Period, if no justification for extension or other exception applies, this data should be deleted or anonymised in accordance with the section of this Policy titled 'Dealing with Personal Data that is No Longer Needed'.

13. SUNK RECORDINGS LTD's Retention Periods are set out in the schedule to this Policy titled 'Schedule - Retention Periods'.

14. The Retention Periods apply however the Personal Data is held by us (e.g. whatever its location or format).

Dealing with Personal Data that is No Longer Needed

15. All Personal Data that is no longer needed in any way must be either deleted (i.e. erased) or anonymised.

16. Deletion of Personal Data held electronically entails this data being permanently deleted as far as is technologically possible. This means that the Staff Member carrying out the deletion must ensure that, after deletion, it is beyond use

(i.e. they must ensure that, if any traces remain, these traces cannot identify the Data Subject). The Staff Member carrying out the deletion should ensure that:

a. Any offline copies of the Personal Data are deleted, as well as published/online versions;

b. Any backup copies of the Personal Data are deleted, whether or not such copies are up-to-date.

17. Deletion of Personal Data held in hard copy entails destruction of this data to the extent that it is beyond use (e.g. so that it cannot be reassembled or read).

18. Anonymisation entails Personal Data being altered into a form that does not allow identification of the Data Subject in any way (i.e. so that the information no longer constitutes Personal Data and is no longer covered by UK Data Protection Laws). Anonymisation may be carried out as an alternative to deletion when useful for the Organisation and appropriate (e.g. for the purposes of carrying out statistical analysis with a large, anonymous dataset).

19. If a Staff Member needs to delete or anonymise Personal Data and they are uncertain as to how to appropriately do so, they should contact the Data Protection Officer via email at dee@sunkrecordings.co.uk for assistance.

Responsibility

20. Day-to-day responsibility for monitoring compliance with this Policy, for setting, evaluating, and adapting data retention practices and this Policy, and for setting, evaluating, and adapting Retention Periods, sits with the Data Protection Officer.

21. All individuals working for or acting on behalf of SUNK RECORDINGS LTD at all levels, including senior managers, officers, employees, consultants, trainees, homeworkers, part-time and fixed-term workers, casual workers, agency workers, volunteers, and interns (collectively '**Staff Members**') should follow this Policy in relation to any Personal Data that they Process. If they have any questions or concerns related to this Policy and their data storage obligations, they should contact the Data Protection Officer via email at dee@sunkrecordings.co.uk.

Changes to the Policy and to Retention Periods

22. This Policy does not form part of any contract of employment or similar and SUNK RECORDINGS LTD may amend it at any time at our absolute discretion.

23. Any changes to the Retention Periods will be made in compliance with the law and a new justification will be provided for each new Retention Period set. Any such changes will be communicated to relevant Staff Members in a timely manner to ensure that practices are adapted accordingly.

24. Retention Periods will be reviewed by the Data Protection Officer (or somebody who the Data Protection Officer has assigned to review the Retention Periods on their behalf and subject to their approval) at least once every 2 years, to ensure that these Retention Periods are still reasonable with regard to any changes to the Personal Data held and to any new laws or guidance relevant to a given Retention Period.

Schedule - Retention Periods

Type of Personal Data	***Description/ Examples***	***Purpose of Processing***	***Retention Period***	***Justification***	***Responsibility***

					y for this Type of Personal Data
Employees' personal information	Name and Address, Contact Information	To keep track of necessary employee information	5 years after the employee is no longer employed	To contact previous employees if necessary and related to	the Data Protection Officer

				their employment	
Staff core payment records	Payroll records for wages and salaries, overtime payment records, and bonuses and expenses payment records	To provide wage payments in order to carry out the employer's obligations under contracts of employment	7 years after the end of the tax year to which the payments relate	In accordance with Taxes Management Act 1970	the Data Protection Officer

INFORMATION SECURITY POLICY

Statement of Policy

1. SUNK RECORDINGS LTD (the **Employer**, **we** or **our**) is committed to the highest standards of information security and treats data security and confidentiality extremely seriously.
2. This Policy and the rules contained in it apply to all staff of the Employer, irrespective of seniority, tenure and working hours, including all employees, directors and officers, consultants and contractors, temporary and agency workers, trainees, casual and fixed-term staff, apprentices, interns and any volunteers (**Staff** or **you**).
3. All Staff must familiarise themselves with this Policy and comply with its terms.

Purpose of Policy

4. In relation to personal data, under the UK General Data Protection Regulation (the **UK GDPR**), the Employer must:
    a. ensure the security of personal data, including protection against any unlawful or unauthorised data processing and accidental loss, damage or destruction, by utilising appropriate technical or organisational measures;
    b. demonstrate the consideration and integration of data compliance measures into the Employer's data processing activities, by implementing appropriate technical or organisational measures; and
    c. be able to demonstrate the use and implementation of such appropriate technical or organisational measures.
5. The purpose of this Policy is to:
    a. protect against any potential breaches of confidentiality;
    b. protect the Employer's informational assets and IT systems and facilities against any loss, damage or misuse;
    c. supplement the Employer's Data Protection and Security Policy in ensuring that Staff are aware of and comply with UK laws and the Employer's policies and procedures on the processing of personal data; and
    d. raise awareness of and clarify the responsibilities and duties of Staff in respect of information security, data security and confidentiality.
6. This is a statement of policy only and does not form part of your contract of employment. The Employer may amend this Policy at any time, in our absolute discretion, and we will do so in accordance with our data protection and other obligations. A new copy of the Policy will be circulated whenever it is changed.
7. For the purposes of this Policy:
    a. **Business Information** means any of the Employer's business-related information other than personal data about customers, clients, suppliers and other business contacts;
    b. **Confidential Information** means any trade secrets or other confidential information (belonging to the Employer or third parties) processed by the Employer;
    c. **Personal Data** means any information that relates to an individual who can be identified from that information, either directly or indirectly; and
    d. **Sensitive Personal Data** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), health, sex life, sexual orientation, genetic information or biometric information (where this is used to identify an individual).

Roles and Responsibilities

8. All Staff have a responsibility for information security. The Employer's Data Protection Officer (DPO) has overall responsibility for this Policy. Specifically, they must:
    a. implement and maintain this Policy;

b. monitor potential and actual security breaches;

c. ensure Staff are aware of their responsibilities in relation to information security and confidentiality; and

d. ensure compliance with the UK GDPR and all other relevant legislation and guidance.

Scope of This Policy

9. This Policy covers all written, verbal and digital information held, used or transmitted by or on behalf of the Employer, irrespective of media. This includes, but is not limited to:

   a. paper records;

   b. hand-held devices;

   c. telephones;

   d. information stored on computer systems; and

   e. information passed on verbally.

10. The information covered by this Policy may include:

   a. Personal Data relating to Staff, customers, clients or suppliers;

   b. other Business Information; and

   c. Confidential Information.

11. This Policy supplements the Employer's Data Protection and Security Policy and other policies relating to data protection, internet, email and communications, and document retention, including the Employer's:

   a. Employee Privacy Notice.

   b. Consultant Privacy Notice.

   c. Data Retention Policy.

   d. Privacy Policy.

   The content of these policies must be considered and taken into account alongside this Policy.

General Principles

12. All information must be:

   a. treated as commercially valuable; and

   b. protected from loss, theft, misuse or inappropriate access or disclosure.

13. Through the use of appropriate technical and organisational measures all Personal Data, including Sensitive Personal Data, must be protected against:

   a. unauthorised and/or unlawful processing; and

   b. accidental loss, destruction or damage.

14. Staff and line managers should discuss what security measures (including technical and organisational measures) are appropriate and which exist to protect any information accessed by Staff in the course of employment.

15. Any information, apart from Personal Data, is owned by the Employer and not by an individual or team.

16. Any information must only be used in connection with work being undertaken for the Employer. It must not be used for any other personal or commercial purposes.

17. Any Personal Data must only be processed for the specified, explicit and legitimate purpose for which it is collected.

Information Management

18. Any Personal Data must be processed in accordance with:

a. the data protection principles;

b. the Employer's policies on data protection generally (including the Data Protection and Security Policy); and

c. the Employer's other relevant policies.

19. All Personal Data collected, used and stored must be:

a. adequate, relevant and limited to what is necessary for the relevant purposes; and

b. kept accurate and up to date.

20. The Employer will take appropriate technical and organisational measures to ensure that Personal Data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage. These measures include:

a. The encryption of Personal Data.

b. The use of strong passwords.

c. Password protection on any documents containing Sensitive Personal Data.

21. Any Personal Data and Confidential Information must not be kept any longer than is necessary and will be stored and destroyed in accordance with our Data Retention Policy.

Human Resources (HR) Information

22. Due to the internal confidentiality of personnel files, access to these files and any information contained therein is limited to the HR Department. Non-HR Staff are not authorised to access HR information, except as provided for in any individual roles.

23. Personnel information must also be kept strictly confidential by any Staff involved in:

a. the recruitment process;

b. a management role; or

c. a supervisory role.

24. Under the UK GDPR and other relevant legislation, Staff may ask to see their personnel files and obtain access to any other Personal Data about them.

Access to Offices and Information

25. All office doors, office keys and access codes must, at all times, be kept secure. Office keys and access codes must at no time be given to or communicated to any third parties.

26. All documents containing and any equipment displaying Confidential Information should be placed and positioned so that anyone passing by cannot see them (e.g. through office windows or glass doors).

27. Any visitors must:

a. sign it at reception;

b. be accompanied by Staff at all times; and

c. not be left alone in areas or situations where they may have access to Confidential Information.

28. Meetings with visitors must, where possible, take place in meeting rooms. If a visitor meeting takes place outside a meeting room, in an office or other room containing Employer information, steps must be taken to ensure no Confidential Information is visible and accessible to the visitors.

29. All paper documents, backup systems and devices containing Confidential Information must be securely locked away:

a. whenever desks are unoccupied; and

b. at the end of the working day.

Computers and IT

30. Where available on our systems, password protection and encryption must be used to maintain confidentiality.

31. All computers and other electronic devices must be password protected. Such passwords must be changed regularly and must not be recorded anywhere (e.g. written down) or made available to others.

32. To minimise the risk of accidental loss or disclosure, all computers and other electronic devices must be locked when not in use, including when left unattended at a desk.

33. All data held electronically must be securely backed up as soon as possible in accordance with the Employer's internal backup procedure.

34. Confidential Information must not be copied onto removable hard drives, CDs or DVDs, floppy disks or memory sticks, without the express permission of the The Data Protection Officer. Any Personal Data held on such devices must, as soon as possible, be transferred to the Employer's computer network to be backed up and then deleted from the device.

35. Staff must:

    a. ensure that they do not introduce viruses, malware or malicious codes onto the Employer's systems.

    b. not install or download from the internet any software without it first being checked for viruses.

    Staff should speak to the The Data Protection Officer for more information and guidance on appropriate steps to be taken to ensure compliance.

Communications and Transfer of Information

36. When speaking in public places (e.g. when speaking on a mobile phone), Staff must take care in maintaining confidentiality.

37. Confidential Information must be marked 'strictly private and confidential' and circulated only to those who need to know the information in the course of their work

38. Confidential Information must not be removed from the Employer's offices (and systems) unless required for authorised business purposes, and then only in accordance with the subsequent paragraph.

39. If the removal of Confidential Information from the Employer's offices is permitted, all reasonable steps must be taken to maintain the confidentiality and integrity of the information. This includes, but is not limited to, Staff ensuring that Confidential Information is:

    a. stored with strong password protection, with devices and files kept locked when not in use;

    b. not transported in see-through or other unsecured bags or cases, when in paper copy;

    c. not read in public places when working remotely (e.g. in waiting rooms or on trains); and

    d. not left unattended or in any place where it is at risk (e.g. in airports or conference centres).

40. Care must be taken to verify all postal and email addresses before any information is sent to them. Particular care must be taken when checking and verifying email addresses where auto-complete features may have inserted incorrect email addresses.

41. Before being sent by email or recorded delivery, all sensitive or particularly confidential information should be encrypted.

Personal Email and Cloud Storage Accounts

42. Personal email accounts (e.g. Google, Hotmail and Yahoo) and cloud storage services (e.g. Google Drive, iCloud and OneDrive) are vulnerable to hacking and do not provide the same level of security as the services provided by the Employer's IT systems.

43. Staff must not use personal email accounts or cloud storage accounts for work purposes.

44. If large amounts of data need to be transferred, Staff should speak to the The Data Protection Officer.

Working From Home

45. Unless required for authorised business purposes, and then only in accordance with the subsequent paragraph, Staff must not take information home with them.

46. Where information is permitted to be taken home, Staff must ensure that appropriate technical and practical measures are in place within the home to maintain the continued security and confidentiality of that information. In particular, all Confidential Information and Personal Data must be:

    a. kept in a secure and locked location, where it cannot be accessed by others (including family members and guests); and

    b. retained and disposed of in accordance with paragraph 21 above.

47. Staff must not store any Confidential Information on their home computers or other devices (e.g. laptops, PCs or tablets).

Transfers to Third Parties

48. Third party service providers should only be engaged to process information where appropriate written agreements are in place to ensure that they offer appropriate data protection, confidentiality and information security protections and undertakings. Care must be taken to consider whether any such third party service providers will be considered data processors for the purpose of the UK GDPR.

49. Staff involved in the process of setting up new arrangements or altering existing arrangements with third parties should speak to and consult with the DPO for more information and guidance.

International Data Transfers

50. There are restrictions on (onward) transfers of Personal Data to international organisations outside of the UK. Staff may only transfer Personal Data outside the UK (including to international organisations outside the UK) if there are sufficient and adequate protections in place. Before making any transfers, Staff should speak to, and seek written authorisation from, the DPO.

51. For more information, see the Employer's Data Protection and Security Policy available from the DPO and online at: https://www.sunkrecordings.co.uk/privacy/. If you have any questions or concerns please contact the DPO or Legal Department.

Training

52. The Employer will provide training on the concepts and measures contained in this Policy to all Staff as part of the induction process and at regular intervals thereafter or whenever there is a substantial change in the law or our policies and procedures.

53. Training is provided by the Data Protection Officer when necessary. The completion of such training is compulsory. The Employer will continually monitor training needs but if you feel that you need further training on any aspect of the relevant law or this Policy, please contact the DPO.

Reporting Data Breaches

54. All Staff are under an obligation to report actual or potential data protection compliance breaches to enable the Employer to:

    a. investigate the breach and take any necessary remedial actions;

    b. maintain a register of compliance breaches; and

    c. make any applicable notifications (e.g. to the Information Commissioner's Office).

55. For more information on the Employer's reporting procedure, contact the DPO.

Consequences of Non-compliance

56. The Employer takes compliance with this Policy very seriously and failure to comply with this Policy puts Staff and the Employer alike at significant risk.

57. Due to the importance of this Policy, failure to comply with any of its procedures and requirements may result in disciplinary action and dismissal.

58. If you have any questions or concerns about anything in this Policy, please contact the DPO at dee@sunkrecordings.co.uk.

Attribution

59. This Information Security Policy was created using a document from Rocket Lawyer (https://www.rocketlawyer.com/gb/en).

PRIVACY POLICY

This Privacy Policy applies between you, the User of this Website, and SUNK RECORDINGS LTD, the owner and provider of this Website. SUNK RECORDINGS LTD takes the privacy of your information very seriously. This Privacy Policy applies to our use of any and all Data collected by us or provided by you in relation to your use of the Website.

Please read this Privacy Policy carefully.

Definitions and Interpretation

1. In this Privacy Policy, the following definitions are used:

Data	collectively all information that you submit to SUNK RECORDINGS LTD via the Website. This definition incorporates, where applicable, the definitions provided in the Data Protection Laws;
Cookies	a small text file placed on your computer by this Website when you visit certain parts of the Website and/or when you use certain features of the Website. Details of the cookies used by this Website are set out in the clause below (**Cookies**);
Data Protection Laws	any applicable law relating to the processing of personal Data, including but not limited to the GDPR, and any national implementing and supplementary laws, regulations and secondary legislation;
GDPR	the UK General Data Protection Regulation;
SUNK RECORDINGS LTD, we or **us**	SUNK RECORDINGS LTD, a company incorporated in Scotland with registered number SC779703 whose registered office is at 3/2 281 St. Georges Road, City of Glasgow, G3 6JQ;
UK and EU Cookie Law	the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 & the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2018;
User or **you**	any third party that accesses the Website and is not either (i) employed by SUNK RECORDINGS LTD and acting in the course of their employment or (ii) engaged as a consultant or otherwise providing services to SUNK RECORDINGS LTD and accessing the Website in connection with the provision of such services; and
Website	the website that you are currently using, www.sunkrecordings.co.uk, and any sub-domains of this site unless expressly excluded by their own terms and conditions.

2. In this Privacy Policy, unless the context requires a different interpretation:
   a. the singular includes the plural and vice versa;
   b. references to sub-clauses, clauses, schedules or appendices are to sub-clauses, clauses, schedules or appendices of this Privacy Policy;
   c. a reference to a person includes firms, companies, government entities, trusts and partnerships;
   d. "including" is understood to mean "including without limitation";
   e. reference to any statutory provision includes any modification or amendment of it;
   f. the headings and sub-headings do not form part of this Privacy Policy.

Scope of this Privacy Policy

3. This Privacy Policy applies only to the actions of SUNK RECORDINGS LTD and Users with respect to this Website. It does not extend to any websites that can be accessed from this Website including, but not limited to, any links we may provide to social media websites.

4. For purposes of the applicable Data Protection Laws, SUNK RECORDINGS LTD is the "data controller". This means that SUNK RECORDINGS LTD determines the purposes for which, and the manner in which, your Data is processed.

Data Collected

5. We may collect the following Data, which includes personal Data, from you:

   a. name;

   b. contact Information such as email addresses and telephone numbers;

   in each case, in accordance with this Privacy Policy.

How We Collect Data

6. We collect Data in the following ways:

   a. data is given to us by you; and

   b. data is collected automatically.

Data That is Given to Us by You

7. SUNK RECORDINGS LTD will collect your Data in a number of ways, for example:

   a. when you contact us through the Website, by telephone, post, e-mail or through any other means;

   b. when you use our services;

   in each case, in accordance with this Privacy Policy.

Data That is Collected Automatically

8. To the extent that you access the Website, we will collect your Data automatically, for example:

   a. we automatically collect some information about your visit to the Website. This information helps us to make improvements to Website content and navigation, and includes your IP address, the date, times and frequency with which you access the Website and the way you use and interact with its content.

   b. we will collect your Data automatically via cookies, in line with the cookie settings on your browser. For more information about cookies, and how we use them on the Website, see the section below, headed "Cookies".

Our Use of Data

9. Any or all of the above Data may be required by us from time to time in order to provide you with the best possible service and experience when using our Website. Specifically, Data may be used by us for the following reasons:

   a. internal record keeping;

   in each case, in accordance with this Privacy Policy.

10. We may use your Data for the above purposes if we deem it necessary to do so for our legitimate interests. If you are not satisfied with this, you have the right to object in certain circumstances (see the section headed "Your rights" below).

11. We may use your Data to show you SUNK RECORDINGS LTD adverts and other content on other websites. If you do not want us to use your data to show you SUNK RECORDINGS LTD adverts and other content on other websites,

please turn off the relevant cookies (please refer to the section headed "Cookies" below).

Who We Share Data With

12. We may share your Data with the following groups of people for the following reasons:

    a. our employees, agents and/or professional advisors - to establish any potential working relationships and obtain advice from professional advisers;

in each case, in accordance with this Privacy Policy.

Keeping Data Secure

13. We will use technical and organisational measures to safeguard your Data, for example:

    a. access to your account is controlled by a password and a user name that is unique to you.

    b. we store your Data on secure servers.

14. Technical and organisational measures include measures to deal with any suspected data breach. If you suspect any misuse or loss or unauthorised access to your Data, please let us know immediately by contacting us via this e-mail address: sunkrecordings@gmail.com.

15. If you want detailed information from Get Safe Online on how to protect your information and your computers and devices against fraud, identity theft, viruses and many other online problems, please visit www.getsafeonline.org. Get Safe Online is supported by HM Government and leading businesses.

Data Retention

16. Unless a longer retention period is required or permitted by law, we will only hold your Data on our systems for the period necessary to fulfil the purposes outlined in this Privacy Policy or until you request that the Data be deleted.

17. Even if we delete your Data, it may persist on backup or archival media for legal, tax or regulatory purposes.

Your Rights

18. You have the following rights in relation to your Data:

    a. **Right to access** - the right to request (i) copies of the information we hold about you at any time, or (ii) that we modify, update or delete such information. If we provide you with access to the information we hold about you, we will not charge you for this, unless your request is "manifestly unfounded or excessive." Where we are legally permitted to do so, we may refuse your request. If we refuse your request, we will tell you the reasons why.

    b. **Right to correct** - the right to have your Data rectified if it is inaccurate or incomplete.

    c. **Right to erase** - the right to request that we delete or remove your Data from our systems.

    d. **Right to restrict our use of your Data** - the right to "block" us from using your Data or limit the way in which we can use it.

    e. **Right to data portability** - the right to request that we move, copy or transfer your Data.

    f. **Right to object** - the right to object to our use of your Data including where we use it for our legitimate interests.

19. To make enquiries, exercise any of your rights set out above, or withdraw your consent to the processing of your Data (where consent is our legal basis for processing your Data), please contact us via this e-mail address: sunkrecordings@gmail.com.

20. If you are not satisfied with the way a complaint you make in relation to your Data is handled by us, you may be able to refer your complaint to the relevant data protection authority. For the UK, this is the Information Commissioner's Office (ICO). The ICO's contact details can be found on their website at https://ico.org.uk/.

21. It is important that the Data we hold about you is accurate and current. Please keep us informed if your Data changes during the period for which we hold it.

Transfers Outside the United Kingdom and European Economic Area

22. Data which we collect from you may be stored and processed in and transferred to countries outside of the UK and European Economic Area (EEA). For example, this could occur if our servers are located in a country outside the UK or EEA or one of our service providers is situated in a country outside the UK or EEA.
23. We will only transfer Data outside the UK or EEA where it is compliant with data protection legislation and the means of transfer provides adequate safeguards in relation to your data, e.g. by way of data transfer agreement, incorporating the current standard contractual clauses adopted by the European Commission.
24. To ensure that your Data receives an adequate level of protection, we have put in place appropriate safeguards and procedures with the third parties we share your Data with. This ensures your Data is treated by those third parties in a way that is consistent with the Data Protection Laws.

Links to Other Websites

25. This Website may, from time to time, provide links to other websites. We have no control over such websites and are not responsible for the content of these websites. This Privacy Policy does not extend to your use of such websites. You are advised to read the Privacy Policy or statement of other websites prior to using them.

Changes of Business Ownership and Control

26. SUNK RECORDINGS LTD may, from time to time, expand or reduce our business and this may involve the sale and/or the transfer of control of all or part of SUNK RECORDINGS LTD. Data provided by Users will, where it is relevant to any part of our business so transferred, be transferred along with that part and the new owner or newly controlling party will, under the terms of this Privacy Policy, be permitted to use the Data for the purposes for which it was originally supplied to us.
27. We may also disclose Data to a prospective purchaser of our business or any part of it.
28. In the above instances, we will take steps with the aim of ensuring your privacy is protected.

Cookies

29. This Website may place and access certain Cookies on your computer. SUNK RECORDINGS LTD uses Cookies to improve your experience of using the Website. SUNK RECORDINGS LTD has carefully chosen these Cookies and has taken steps to ensure that your privacy is protected and respected at all times.
30. All Cookies used by this Website are used in accordance with current UK and EU Cookie Law.
31. Before the Website places Cookies on your computer, you will be presented with a message bar requesting your consent to set those Cookies. By giving your consent to the placing of Cookies, you are enabling SUNK RECORDINGS LTD to provide a better experience and service to you. You may, if you wish, deny consent to the placing of Cookies; however certain features of the Website may not function fully or as intended.
32. This Website may place the following Cookies:

Type of Cookie	Purpose
Strictly necessary cookies	These are cookies that are required for the operation of our website. They include, for example, cookies that enable you to log into secure areas of our website, use a shopping cart or make use of e-billing services.

Analytical/performance cookies	They allow us to recognise and count the number of visitors and to see how visitors move around our website when they are using it. This helps us to improve the way our website works, for example, by ensuring that users are finding what they are looking for easily.
Functionality cookies	These are used to recognise you when you return to our website. This enables us to personalise our content for you, greet you by name and remember your preferences (for example, your choice of language or region). By using the Website, you agree to our placement of functionality cookie.
Targeting cookies	These cookies record your visit to our website, the pages you have visited and the links you have followed. We will use this information to make our website and the advertising displayed on it more relevant to your interests. We may also share this information with third parties for this purpose.

33. You can find a list of Cookies that we use in the Cookies Schedule.

34. We give you control over which Cookies we use. You can adjust your cookies preferences at any time at: sunkrecordings.co.uk.

35. You can also choose to enable or disable Cookies in your internet browser. By default, most internet browsers accept Cookies but this can be changed. For further details, please see the help menu in your internet browser. You can switch off Cookies at any time, however, you may lose any information that enables you to access the Website more quickly and efficiently.

36. You can choose to delete Cookies at any time; however, you may lose any information that enables you to access the Website more quickly and efficiently including, but not limited to, personalisation settings.

37. It is recommended that you ensure that your internet browser is up-to-date and that you consult the help and guidance provided by the developer of your internet browser if you are unsure about adjusting your privacy settings.

38. For more information generally on cookies, including how to disable them, please refer to aboutcookies.org. You will also find details on how to delete cookies from your computer.

General

39. You may not transfer any of your rights under this Privacy Policy to any other person. We may transfer our rights under this Privacy Policy where we reasonably believe your rights will not be affected.

40. If any court or competent authority finds that any provision of this Privacy Policy (or part of any provision) is invalid, illegal or unenforceable, that provision or part-provision will, to the extent required, be deemed to be deleted, and the validity and enforceability of the other provisions of this Privacy Policy will not be affected.

41. Unless otherwise agreed, no delay, act or omission by a party in exercising any right or remedy will be deemed a waiver of that, or any other, right or remedy.

42. This Agreement will be governed by and interpreted according to the law of Scotland. All disputes arising under the Agreement will be subject to the exclusive jurisdiction of the Scottish.

Changes to This Privacy Policy

43. SUNK RECORDINGS LTD reserves the right to change this Privacy Policy as we may deem necessary from time to time or as may be required by law. Any changes will be immediately posted on the Website and you are deemed to have accepted the terms of the Privacy Policy on your first use of the Website following the alterations.

You may contact SUNK RECORDINGS LTD by email at sunkrecordings@gmail.com.

Attribution

44. This Privacy Policy was created using a document from Rocket Lawyer (https://www.rocketlawyer.com/gb/en).

This Privacy Policy was created on **09 September 2025**.

Cookies

Below is a list of the cookies that we use. We have tried to ensure this is complete and up to date, but if you think that we have missed a cookie or there is any discrepancy, please let us know.

Strictly necessary

We use the following strictly necessary cookies:

Description	Purpose
Necessary	Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Functionality

We use the following functionality cookies:

Description	Purpose
Preferences	Preference cookies enable a website to remember information that changes the way the website behaves or looks, like your preferred language or the region that you are in.

Analytical/Performance

We use the following analytical/performance cookies:

Description	Purpose
Statistics	Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting information anonymously.

Targeting

We use the following targeting cookies:

Description	Purpose
Marketing Unclassified	Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers. Unclassified cookies are cookies that we are in the process of classifying, together with the providers of individual cookies.