



**Privacy policy for employees, workers,  
independent contractors, trustees and volunteers**

**1. What is the purpose of this document?**

Les Crocodiles (charity incorporated organisation (CIO) entered in the Register of Charities at the Charity Commission under the charity number 1158669 with a registered office address of Flat 1203, Moro Apartments, 22 New Festival Avenue, London, E14 6FT) ("**Les Crocodiles**") is committed to protecting the privacy and security of your personal information.

Les Crocodiles is a "controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Privacy Policy. This Privacy Policy describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the UK General Data Protection Regulation ("**UK GDPR**") and other applicable data protection legislation. This privacy policy applies to all employees, workers, independent contractors (including teachers, assistants and any self-employed individuals).

We may update this Privacy Policy at any time but if we do so, we will provide you with an updated copy of this privacy policy as soon as reasonably practical. This Privacy Policy was last updated on 25 April 2024.

It is important that you read and retain this Privacy Policy, together with any other privacy policy we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using that information and what your rights are under the data protection legislation.

**If you have any questions about this Privacy Policy, please contact us at [privacy@les-crocodiles.org](mailto:privacy@les-crocodiles.org).**

**2. Data protection principles**

We will comply with data protection legislation, which says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

### **3. The kind of information we hold about you**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the person's identity has been removed (anonymous data).

There are certain types of more sensitive personal data which require a higher level of protection, such as information about a person's health, sexual orientation or criminal convictions.

We will collect, store and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers and personal email addresses.
- Date of birth.
- Gender.
- National Insurance number (when applicable).
- Bank account details.
- Salary, annual leave, pension and benefits information (when applicable).
- Start date and, if different, the date of commencement of your working relationship with us.
- Termination date of your employment or contract with us and your reason for leaving.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Compensation history.
- Performance information.
- Information about your use of our information and communications systems.
- Files and training records created by you.
- Minutes of meetings you attend and email messages with you.

We may also collect, store and use the following more sensitive types of personal information:

- Information about your health, including any medical condition and sickness records, including details of any absences (other than holidays) from work.
- Information about criminal convictions and offences.

### **4. How is your personal information collected?**

#### Employees, workers, and independent contractors

We collect personal information about employees, workers, and independent contractors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies. We will collect additional personal information throughout your working relationship with us.

## Trustees and volunteers

We collect personal information about trustees and volunteers directly from our interactions with you. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies, as are relevant to your role and relationship with us.

We will collect additional personal information throughout your relationship with us.

### **5. How we will use information about you**

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to **perform the contract** we have entered into with you.
2. Where we need to **comply with a legal obligation**.
3. Where it is necessary for **legitimate interests** pursued by us or a third party and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.
3. Where you have given your consent for us to do so.

### **6. Situations in which we will use your personal information**

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below.

## Employees, workers, and independent contractors

- Making a decision about your recruitment or appointment.
- Paying you and, if you are an employee or deemed employee for tax purposes, deducting tax and National Insurance contributions (NICs).
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Assessing qualifications, training and development requirements.
- Gathering evidence for possible capability, grievance or disciplinary hearings and conducting such hearings or related procedures.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.

- Dealing with legal disputes involving you, or other employees, workers, independent contractors, trustees or volunteers including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- To provide references.
- To maintain appropriate human resources records for current and former employees, workers, and independent contractors.
- Equal opportunities monitoring.

#### Trustees and volunteers

- Making a decision about your appointment.
- Administering the contract we have entered into with you (if applicable).
- Business management and planning, including accounting and auditing.
- Assessing qualifications, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers, independent contractors, trustees or volunteers including accidents at work.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.

### **7. If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### **8. Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose.

If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **9. How we use particularly sensitive personal information**

Special categories of particularly sensitive personal information, such as information about your health, racial or ethnic origin, sexual orientation, or trade union membership, require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

## **10. Situations in which we will use your sensitive personal information**

In general, we will not process particularly sensitive personal information about you unless it is necessary for performing or exercising obligations or rights in connection with employment or your engagement with us. On rare occasions, there may be other reasons for processing, such as it is in the public interest to do so. We will inform you in the event that we need to process any sensitive personal information about you.

## **11. Do we need your consent?**

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

We do not need your consent where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.

## **12. Information about criminal convictions**

We envisage that we will hold information about criminal convictions. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working with us.

We will use information about criminal convictions and offences to conduct Disclosure and Barring Service (“DBS”) checks on all independent contractors and on all individuals with regular contact with children prior to offering a role to work with us in accordance with our [Safeguarding Policy](#). We conduct Enhanced with Barred Lists DBS checks. We record the date of the DBS check, the number of the DBS check and the name conducting the DBS check as well as the result of the DBS check and retain this for two years. The “appropriate policy document” contained in Schedule 1 supplements this Privacy Policy with respect to the processing of information about criminal convictions and meets the requirement of the Data Protection Act

2018 that an appropriate policy document be in place where processing information about criminal convictions in certain circumstances. We have in place safeguards which we are required by law to maintain when processing such data.

### **13. Automated decision-making**

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you. We do not envisage that any decisions will be taken about you using automated means. However, we will notify you in writing if this position changes.

### **14. Data sharing**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. Third parties includes third-party service providers (including contractors and designated agents). The following third-party service providers process personal information about you for the following purposes:

- Salesforce, for the management of contracts;
- Microsoft Office 365, for emails, cloud storage, collaboration, and document production;
- Typeform, for document production;
- Waterbear, for the library software at the school; and
- QuickFile, for accounting and invoicing purposes.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

We may share your personal information with other third parties, in exceptional circumstances. We will, so far as possible, share anonymised data with the other parties.

We may also need to share your personal information with a regulator or to otherwise comply with the law. This may include making returns to HMRC.

### **15. International transfers**

Where we transfer your personal data outside of the UK, we ensure that a similar degree of protection is afforded to it by ensuring that (i) we will only transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data, or (ii) we may use specific contracts approved for use in the UK which give personal data the same protection it has in the UK.

### **16. Data security**

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Additionally, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **17. Data retention**

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including for the purposes of satisfying any legal, accounting or reporting requirements. Details of retention periods for different aspects of your personal information are available in our Retention Policy which is available from the DPO.

To determine the appropriate retention period for personal data, we consider:

- The amount, nature and sensitivity of the personal data.
- The potential risk of harm from unauthorised use or disclosure of your personal data.
- The purposes for which we process your personal data and whether we can achieve those purposes through other means.
- The applicable legal requirements.

In some circumstances, we may anonymise your personal information so that it can no longer be associated with you, in which case we may use that information without further notice to you. Once you are no longer an employee, worker, independent contractor, trustee or volunteer for Les Crocodiles, we will retain and securely destroy your personal information in accordance with our Retention Policy.

## **18. Your legal rights**

### **Your duty to inform us of changes**

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

### **Your rights in connection with personal data**

Under certain circumstances, by law you have the right to:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes.

- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact us at the email address at Section 1 above.

#### **No fee usually required**

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in these circumstances.

#### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

#### **Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact us at the email address at Section 1 above. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

#### **19. Data protection officer (“DPO”)**

We have appointed a DPO to oversee compliance with this Privacy Policy. If you have any questions about this Privacy Policy or how we handle your personal information, please contact the DPO. The DPO can be contacted by email at [dpo@les-crocodiles.org](mailto:dpo@les-crocodiles.org).

You have the right to make a complaint at any time to the Information Commissioner's Office (“ICO”) with respect to data protection issues.



## Schedule 1 - Appropriate Policy Document (Information about Criminal Convictions)

### 1. About this Schedule

This is the "appropriate policy document" for Les Crocodiles (charity incorporated organisation (CIO) entered in the Register of Charities at the Charity Commission under the charity number 1158669 with a registered office address of Flat 1203, Moro Apartments, 22 New Festival Avenue, London, E14 6FT) ("**Les Crocodiles**") setting out how we will protect criminal offence data. "**Criminal offence data**" as used in this Schedule consists of personal data relating to criminal convictions and offences or related security measures.

This Schedule supports our privacy policy for employees, workers, independent contractors, trustees and volunteers and adopts its definitions.

This document meets the requirement of the Data Protection Act 2018 ("**DPA 2018**") that an appropriate policy document be in place for the processing of criminal offence data in certain circumstances.

### 2. Why we process criminal offence data

We process criminal offence data to assess applicants' suitability to work or volunteer in positions where the safeguarding of children and individuals at risk must be ensured.

### 3. Personal data protection principles

The UK General Data Protection Regulation ("**UK GDPR**") requires personal data to be processed in accordance with the six principles set out in Article 5(1). Article 5(2) requires controllers to be able to demonstrate compliance with Article 5(1).

We comply with the principles relating to processing of personal data set out in the UK GDPR. The principles require personal data to be:

- processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);
- collected only for specified, explicit and legitimate purposes (**purpose limitation**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (**data minimisation**);
- accurate and where necessary kept up to date (**accuracy**);
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (**storage limitation**);
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**security, integrity and confidentiality**);
- not transferred to another country without appropriate safeguards in place (**transfer limitation**); and
- made available to data subjects and allow data subjects to exercise certain rights in relation to their personal data (**data subject's rights and requests**).

### 4. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We will only process personal data fairly and lawfully and for specified purposes. The UK GDPR restricts our actions regarding personal data to specified lawful purposes. We can process criminal offence data

only if we have a legal ground for processing and one of the specific processing conditions relating to criminal offence data applies. We will identify and document the legal ground and specific processing condition relied on for each processing activity.

When collecting criminal offence data from data subjects, either directly from data subjects or indirectly (for example from a third party or publicly available source), we will provide data subjects with a privacy policy setting out all the information required by the UK GDPR in a privacy policy which is concise, transparent, intelligible, easily accessible and in clear plain language which can be easily understood.

Lawful processing basis	Processing condition for criminal offence data
Processing is necessary for the purposes of the legitimate interests pursued by the controller ( <i>Article 6(1)(f) UK GDPR</i> ).	Necessary for the purposes of safeguarding of children and of individuals at risk ( <i>Paragraph 18, Schedule 1, DPA 2018</i> ).

## 5. Storage limitation

We only keep criminal offence data in an identifiable form for as long as is necessary for the purposes for which it was collected or where we have a legal obligation to do so. Once we no longer need the criminal offence data it shall be deleted or rendered permanently anonymous.

We will ensure data subjects are informed of the period for which personal data is stored and how that period is determined in our privacy policy.

## 6. Policies on retention and erasure of personal data

We take the security of criminal offence data very seriously. We have administrative, physical and technical safeguards in place to protect criminal offence data against unlawful or unauthorised processing, or accidental loss or damage. We will ensure, where criminal offence data is processed that:

- The processing is recorded, and the record sets out, where possible, a suitable time period for the safe and permanent erasure of the data in accordance with our retention policies.
- Where we no longer require criminal offence data for the purpose for which it was collected, we will delete it or render it permanently anonymous as soon as possible.
- Where records are destroyed we will ensure that they are safely and permanently disposed of.

Data subjects receive a privacy policy setting out how their personal data will be handled when we first obtain their personal data, and this will include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

## 7. Review

This Schedule on processing criminal offence data is reviewed annually.

The Schedule will be retained where we process criminal offence data and for a period of at least six months after we stop carrying out such processing.

A copy of this Schedule will be provided to the Information Commissioner on request and free of charge.