SUFFOLK ARCHAEOLOGY

General Data Protection Regulation Policy

1 Introduction

Suffolk Archaeology CIC holds information which has to be managed in accordance with the General Data Protection Regulation (GDPR). This policy describes the actions we take to ensure compliance with the policy.

We recognise that it is not our data to use as we wish, but it is your data that we are merely custodians of. We fully respect that you have entrusted your data with us and we will take care to ensure that your data is fully protected.

This policy ensures we:

- comply with data protection law and follow sound practice
- ensure the rights of staff, customers, and business partners are adhered to
- are open about the way we process and manage information
- reduce the risk of a data breach
- are able to respond quickly in the event of a breach

2 Scope

This policy applies to all Suffolk Archaeology's activities irrespective of location, all staff, and direct contractors.

3 Why we hold data?

We hold personal data and sensitive personal data to enable us to:

- manage our employees
- provide Archaeological services to our customers
- manage the health and safety of our customers and our staff
- manage our volunteers
- make information available to volunteers and other interested people via our newsletters

4 What basis do we hold and process data?

We will only use personal information for lawful business purposes set out under the GDPR.

Wherever possible we will not rely on consent to hold data; we will identify another ground to justify holding data.

We will only hold and process data on the basis that we have explained; We will not seek to process data in a way which is different from the original intent.

5 Sensitive Personal Data

We will not hold or process sensitive personal information unless the security and management arrangements of the GDPR higher standards have been met.

We will undertake a Data Protection Impact Assessment (DPIA) and Risk Assessment to determine the appropriate measures to be taken to protect any Sensitive Personal Data that we hold or process.

6 Children

At Suffolk Archaeology we hold data about children for work experience purposes only. We will undertake a Data Protection Impact Assessment (DPIA) and Risk Assessment to determine the appropriate measures to be taken to protect any data regarding children that we hold.

7 Notices

We will be open, accurate, and clear in explaining how personal data will be used.

Notices will be made available to staff, and to customers & guests via a notice on our web site.

8 Individuals Rights

We will provide requested data as promptly as we can, and in accordance with timescales set out under the GDPR.

Processes for contacting us to request data that we hold will be clearly available and easy to understand.

We aim to acknowledge all requests for data within 24 hours.

9 Data Management

9.1 Minimisation of Data

We will hold the minimum amount of data that is necessary for the function of our business.

9.2 Accuracy

We will keep information up to date and correct any inaccurate data that is identified.

9.3 Retention of Data

We will only hold data longer than standard retention guidelines for public interest reasons, for contributing to and the enhancement of the historical record.

Our information retention policy is located in the Appendix.

9.4 Transferring Data Overseas

We will not export your data overseas without ensuring appropriate data protection arrangements are in place.

SUFFOLK ARCHAEOLOGY

9.5 Automated Decision Making

We will not use automated decision making solely when making a decision which will have a direct impact on an individual.

10 Protective Measures

10.1 Security of Data

We will ensure that we apply appropriate industry standard security measures when securing and handling personal data.

We will take specialist advice, where necessary, to ensure our security measures are providing the expected level of protection.

10.2 Incident Reporting

We will treat all security incidents as a serious matter and provide appropriate resources to their investigation.

We will report security incidents as required by the GDPR and the Information Commissioner's Office (ICO).

Staff and direct contractors are required to report any incidents or breaches of this policy as soon as possible.

Any findings as a result of a security incident will be used to improve our systems, processes, and training.

10.3 New Systems and Processes

We will ensure privacy is considered at the outset of any new information processing systems and business processes.

10.4 Third Parties We Work With

Depending on the type of supplier, we undertake one of the following:

- review their terms and conditions to ensure they protect data in accordance with GDPR requirements
- provide details of the information we hold and process, ensure they understand their responsibilities in helping us secure it, and formally agree the arrangements

11 Direct Marketing

When obtaining marketing data, we will ensure it is from a GDPR compliant supplier.

11.1 Business to Business (B2B)

We will ensure that B2B marketing communications have a clear method of opting out of further communications from us.

We will take care when adding details to our mailing lists to ensure we treat sole traders and partnerships as Business to Client (B2C) parties.

SUFFOLK ARCHAEOLOGY

11.2 Business to Client (B2C)

We will ensure we gain consent prior to adding you to our mailing list.

We will ensure that B2C marketing communications have a clear method of opting out of further communications from us.

12 Complaints

We will investigate complaints or disputes conceding the holding or processing of personal data promptly

If necessary, we will cooperate with the ICO in the investigation and resolution of complaints and will aim to comply with any recommendations.

13 Compliance

13.1 Failures

Failure to comply with this policy by staff will be dealt with under our disciplinary procedures.

Failure to comply with this policy by direct contractors will be dealt with under the terms of the contract between us, which could include termination.

13.2 Training

We will train our staff on the GDPR and provide refresher training as required.

14 Accountability

We will have documentary evidence to support our GDPR compliance, including:

- analysis of data types and their flows
- the locations (logical and physical) where data is held
- the people with access to the information
- assessment of the suitability of the security controls applied
- details of arrangements we have with our suppliers to maintain protection

SUFFOLK ARCHAEOLOGY

15 Appendix A - Information Retention Policy

15.1 Internal Documents

	Document	Retention Period	Notes
	Personnel Records for Senior Executives	Six years	Some records may be required for historical purposes.
	Employee Personnel Records	Six years after ending employment	There is a six-year limitation period for civil claims.
	Applications for jobs where the candidate is unsuccessful	One year after notifying candidate	There is a one-year limit to claim defamation under the Equality Act 2010
	Payroll Records	Six years from the year end for limited companies Unincorporated companies – five years after the January 31st of the following year of assessment	
	PAYE records	Six years	
	National Minimum Wage	Three years after the end of pay reference period	National Minimum Wage Act 1998
	Salary Registers and Revisions	Five years	
	Statutory Maternity Pay Records	Three years after the tax year which they cover	
	HMRC Approvals	Permanently	
	Pension Records	Twelve years after benefits paid.	
	Expenses	Six years	
	Drivers' log books	Five years	
	Vehicle records: Mileage, Maintenance, MoT, & Registration Records	Two years after vehicle disposal	

	Accident Book	Keep each entry for twelve years	
	Health and Safety Reports	Permanently	
	Health & Safety Records	Personal injury claims – three years Industrial injuries caused by hazardous substances – 40 years	
	Accident Reports and Insurance Correspondence	Six years following case closure	
	Assessments under health and safety law for consultation with safety representatives	Permanently	
	Employers Liability Insurance Certificate Records	Permanently	
	Sickness Records	Three years after the tax year which they cover for SSP purposes	
	Paternity and Parental Leave Records	Five years form birth or adoption. Eighteen years if the child is disabled.	
	Time booking records	Two years	
	Working Time Records	Two years	
	Children in Work Records	Until the child reaches 21.	
	Training records	Fifteen Years	
	Trade Union Collective Agreements	Ten years	
	Works council minutes	Permanently	
	Patent Agreements with Staff	20 years after employment ends	

SUFFOLK ARCHAEOLOGY

15.2 Supplier/Customer Documents

	Document	Retention Period	Notes
	Invoices/orders/financial information	6 years	As per **www.gov.uk**
	Contracts	Permanently within archive	Records may be kept for historical purposes
	Site data (including archaeological site reports)	Permanently within archive	Records may be kept for historical purposes