DATA PROTECTION POLICY

Coram and is required by law to comply with the **Data Protection Act, 1998**. It is the commitment of this organisation to ensure that every current member of staff complies with this Act to ensure the confidentiality of any personal data held by Coram, in whatever medium. This Act came into force on 1st March 2000.

In this document the use of Coram is used to apply to all members of the Coram Group of charities.

The Data Protection Act 1998, [the Act], covers all personal data held on electronic systems and on all forms of media (including, but not limited to paper, microfilm and electronic media).

1. Introduction

Coram needs to keep certain information about its staff, service users, and other users of Coram facilities and services for a number of legitimate business purposes. It is therefore highly likely that in the course of your employment you will come into contact with or use confidential information about employees, clients or service users.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this Coram must comply with the eight Data Protection Principles which are set out in the Act. In summary these state that personal data shall be:

1. Processed fairly and lawfully and shall not be processed unless certain conditions are met.

2. Obtained for specified and lawful purposes and not further processed in a manner incompatible with these purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date
5. Kept for no longer than necessary.
6. Processed in accordance with data subjects' rights.
7. Protected by appropriate technical and organisational security.
8. Not transferred to countries outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

All Coram employees, sessionals, volunteers, associates, students and others who process or use any personal information have a duty to ensure that they follow these principles at all times. In order to ensure that this happens, Coram has developed this Data Protection Policy.

Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken, access to Coram facilities being withdrawn, and even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Coram Data Protection Officer (Julia Roper, Human Resources Advisor).

Staff also have obligations to inform Coram of changes to their personal information and have rights to know about and to access information held on them by Coram.

2. Definitions

It is likely that most information about workers that is processed by an organisation will fall within the scope of the Data Protection Act.

Personal Data is defined in the Act as data that:

- relates to a living individual, and
- identifies an individual on its own or when taken together with other information that is in the organisation's possession or that is likely to come into its possession.
- This includes any expression of opinion about the individual and any indications of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data is defined in the Act as personal data consisting of information as to:

- The racial or ethnic origin of the individual
- His/her political opinions
- His/her religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union
- His/her physical or mental health or condition (the definition of health is considered broadly under the Act; it is not defined exhaustively but includes preventative medicine, medical diagnosis, DNA sequences, medical research, provision of care and treatment and the management of healthcare services.)
- His/her sexual life
- The commission or alleged commission by him/her of any offence

- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Personal demographic data are also considered to be sensitive (e.g. home address, salary, and bank financial details).

Examples of sensitive personal data that may typically be found on an employee's record include information relating to their:

- Physical and mental health as part of the sickness records necessary for payment of SSP;
- Disabilities – to facilitate reasonable adjustments in the workplace;
- Ethnic origin – to support the organisation's commitment to equality of opportunity;
- Trade union membership – to enable deduction of subscriptions via the payroll.

The Act applies to personal data that are subject to ***processing***. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities, including the initial obtaining of personal data, its keeping and use, accessing and disclosure, through to their final destruction. In practice, nearly all useable information held about individual workers will be covered by the Act.

3. Responsibilities for Data Protection

Senior Management Team
The Coram Group, as a collection of corporate bodies, has number of Data Controllers as defined under the Act. Details of data controllers, registration numbers and expiry dates are set out in the table below. The Senior Management Team(s), on behalf of the Board(s) of Trustees, as the governing bodies of the Coram Group, are ultimately responsible for the implementation of the Act. Dr. Carol Homden, Chief Executive, is the named contact for all correspondence with the Information Commissioner's Office. As such, the CEO (or her nominated representative) is responsible for ensuring that the Coram Data Protection Registration is kept up to date.

Data Controller	Registration Number	Annual expiry date
Coram	Z6086079	1st January
Coram Children's Legal Centre	Z5589178	22nd July
Voice for the Child in Care	Z1771502	20th May
The Foundling Museum	Z3046338	1st March

Data Protection Officer (DPO)
The Coram Data Protection Officer is Christine Kelly (e-mail: dataprotection@coram.org.uk). The Coram DPO will disseminate information about any changes or amendments to the Act, and advise on the implementation of the Act. The Coram DPO shall investigate reported losses of personal information, calling upon technical support as needed.

Heads of Service
Each Coram Head of Service (or their nominated representative(s)) or Managing Director is responsible for their service's compliance with the Data Protection Act and for ensuring that the

personal data held by their service is kept securely and used properly, within the terms of the Act. Each Head of Service (or their nominee) or Managing Director is responsible for:

- Ascertaining that appropriate technical and organisational measures are taken within their service to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data, in accordance with Coram policies.
- Reporting any loss of personal data to the Data Protection Officer.

All Staff
All staff are responsible for ensuring that any personal data which they own, manage, process or otherwise access, in whatever form (e.g. electronic, microfilm, paper, etc.), is kept securely, in accordance with this policy, the Information Security Policy and the Records Management Policy.

Staff whose work includes responsibility for supervision of volunteers, interns or students, have a duty to ensure that they observe the eight principles of the Act.

Staff must ensure that they are familiar with the Data Protection Policy and must comply with the requirements of section 4 ('Handling of personal data'). Any breach of the Data Protection Policy, either deliberate or through negligence, may lead to disciplinary action being taken, or access to Coram facilities being withdrawn, and even a criminal prosecution. Accessing another employee's records without authority constitutes gross misconduct and could lead to your summary dismissal. It is also a criminal offence under s.55 of the Act.

All staff are responsible for ensuring that personal information is not disclosed orally or in writing or otherwise, either accidentally or otherwise to any unauthorised third party. They must ensure that any transfer to third parties is authorised, lawful and uses appropriate, safe transport mechanisms (e.g. strong encryption).

4. Handling of Personal Data

You should ensure you comply with the following guidelines at all times:

4.1 Do not give out confidential personal information except to the data subject. In particular, it should not be given to someone from the same family or to any other unauthorised third party unless the data subject has given their explicit consent to this.

4.2 If you receive a request for personal information about another employee, you should forward this to Human Resources, who will be responsible for dealing with such requests.

4.3 Be aware that those seeking information sometimes use deception in order to gain access to it. Always verify the identity of the data subject and the legitimacy of the request, particularly before releasing personal information by telephone.

4.4 Transfer of personal data to third parties must be authorised by the Head of Service (or their nominee) or the Managing Director and must use safe transport mechanisms (e.g. strong encryption). Any information transmitted using this form of communication must be clearly

marked 'Private & Confidential' and you must ensure that the individual is able to receive such information confidentially.

4.4 Downloading of any personal data onto mobile devices (such as laptops, mobile phones and iPods), removable devices (such as USB drives, CDs, and DVDs), or any computer not owned by Coram must be authorised by the Head of Service (or their nominee) or Managing Director in writing. The Head of Service or Managing Director must confirm that the volume and sensitivity of the data are proportionate to the business need. Downloaded data and any personal data products must be strongly encrypted. The IT Team can offer guidance on what constitutes an acceptable standard of encryption.

4.5 To avoid loss of encrypted data, an unencrypted copy of the data must be held in a secure environment.

4.6 Staff responsible for handling personal data should consider whether remote access to Coram server(s) using secure connections offers a lower risk solution than downloading personal data.

4.7 Ensure any personal data you hold is kept securely, either in a locked filing cabinet or, if kept electronically, it is password protected.

4.8 Do not retain information for anything other than what it is needed. For example, you do not need to keep additional copies of references or application forms as these are kept within HR.

4.9 All losses of personal data must be reported to the Head of Service and Coram Data Protection Officer. Coram must consider whether or not to report the incident to the Information Commissioner's Office (the independent body who makes sure organisations fulfil their legal obligations under the Act). There is an expectation that a breach involving sensitive personal data should be reported.

4.10 Staff responsible for obtaining personal data from Coram service users must ensure that:

- Each individual is informed of why their personal details are required and consents to their personal information being used.
- All information is kept securely in accordance with the Coram information security policy.
- Data received from third party organisations should be anonymised before receipt or should be accompanied by a signed declaration from the Head of the organisation that it has been collected in accordance with the Act.
- Data to be shared with a third party organisation should, if possible, by anonymised before transfer.
- Personal Data should not be shared with a third party organisation unless the Head of the organisation provides a signed declaration undertaking to use the Data in accordance with the Act.
- The Data Protection Officer must be informed of all agreements regarding the transfer of personal data, to ensure that they comply with the Act and the Coram Data Protection requirements.

- Personal data must be stored and disposed of in accordance with the Act and the Coram Records Management Policy

4.11 Incoming and Internal Post:

Items which are marked 'Personal' or 'Private and Confidential', or which appear to be of a personal nature, should be opened by the addressee only, or by that person's nominated representative. Unless postal items are marked in this way they will be presumed not to contain confidential information, as designated by the Data Protection Act (1998). Staff are discouraged from using their Coram address for non-Coram matters.

4.12 Any member of Coram staff receiving a request for information from a representative of a law enforcement agency (including requests supported by a warrant) should refer the request immediately to the Coram Data Protection Officer. The DPO is best placed to check the validity of warrants. Staff disclosing personal data may not be protected by an invalid warrant.

4.13 No workers should disclose personal data outside the organisation's procedures, or use personal data held on others for their own purposes.

4.14 All staff involved in the processing of personal data must contact the Coram Data Protection Officer if they are in any doubt about what they must or must not do when handling personal data.

4.15 Compliance with the Act is your responsibility.

5. Subject Consent to Processing Sensitive Information

5.1 Unless the law allows it or in exceptional circumstances Coram can only process personal data with the consent of the individual. If the data is sensitive, explicit consent must be obtained, unless there are exceptional circumstances. Agreement to Coram processing some specified classes of personal data is a condition of employment for staff and should be a condition of acceptance for any individual wishing to access Coram services.

5.2 Coram may ask for information about a person's health or disability in relation to their work or standing. Coram may also ask for information such as a person's criminal convictions, ethnicity, sex, and family details. This is to ensure that Coram is a safe place for everyone, or to operate other Coram policies (such as the sick pay policy or equal opportunities policy) or to comply with legal obligations, e.g. under the Children Act 2004.

5.3 By signing your contract of employment you give your explicit consent to Coram holding and processing sensitive personal data, for example, sickness absence records, health needs and equal opportunities monitoring data. Offers of employment may be withdrawn if an individual refuses to consent to this, without good reason.

5.4 We monitor emails and telephone calls but strictly in accordance with what is permitted under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. You have consented to this by a term in your employment contract. Coram

policy relating to monitoring of computer and network usage and how it relates to Coram's data protection policy can be found in the IT policy.

6. Rights to Access Personal Information

6.1 Under the right of subject access an individual is entitled to see their own personal data. All data subjects including employees, sessionals, volunteers, associates, students, and other users of Coram facilities or services are entitled to know:

- what personal information Coram holds and processes about them and why.
- how to gain access to it.
- how to keep it up to date.
- what Coram is doing to comply with its obligations under the 1998 Act.

A list of the types of personal information held about staff by Human Resources will be given, on request, by that department.

6.2 All data subjects including employees, sessionals, volunteers, associates, students, and other users of Coram facilities or services staff, have the right to access any personal data that is being kept about them. Any person who wishes to exercise this right should make their request in writing, using the Coram 'Request for Access to Personal Data'; form (Appendix A) and forward it to the Data Protection Officer. The form must be accompanied by the fee of £10.00 (the amount laid down in the legislation) and proof of ID / residency. Coram has discretion to waive this fee. Coram Voice will waiver this fee where it is a young person who has used their services wanted to access their personal data

6.3 Coram aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

6.4 Coram need not comply with the request for information if doing so would disclose information relating to another individual who could be identified from that information unless the individual has consented to the disclosure or it is reasonable in all the circumstances to provide the information without the consent of the individual. For example, confidential references.

6.5 Coram does not need to comply with a written request where we have already complied with a similar request from the data subject unless a reasonable interval has elapsed between requests.

7. Complaints

If you wish to make a complaint that these rules are not being followed in respect of personal data Coram holds about you, you should raise the matter with the Data Protection Officer. If the matter is not resolved to your satisfaction, it should be raised as a formal grievance under Coram's grievance policy and procedure. If you are still not happy you can appeal to the ICO

who oversees compliance with the Data Protection Act and has a duty to investigate any complaint.

8. Retention of Data

8.1 The Retention of Data Policy applies to all administrative records, whatever their format. All departments within Coram are expected to consult the Head of Service or Managing Directors before disposing of non-current records.

8.2 Coram keeps some forms of information for longer than others, in line with financial, legal, or archival requirements. Coram follows the retention periods recommended by the Information Commissioner in its Employment Practices Data Protection Code.

You should therefore treat the following as guidelines for retention times in the absence of a specific business case supporting a longer period. This list is not exhaustive and advice should always be sought before destroying any information.

Record	Retention Period
Application form	Duration of employment
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Maternity records	3 years after the end of the tax year in which the maternity period ends
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, e.g. name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years
Health & Safety Assessments	Permanently
Redundancy details	6 years from date of redundancy
Senior Executive Records	Permanently
Trade Union Agreements	10 years after ceasing

Any data which Coram decides it does not need to hold for a specific period of time will be destroyed after one year. Data relating to unsuccessful job applicants will only be retained for a period of one year.

All projects are responsible for establishing the retention periods for the documentation that they work with. It is the project's responsibility to ensure that any information to be disposed of is done so in a confidential manner.

9. Obligations to keep Coram's Information up to date

9.1 All staff are responsible for:

- Ensuring that any information that they provide in connection with their employment is accurate and up to date.
- Informing Human Resources and their department of any changes to information which they have provided, e.g. changes of address.
- Informing Human Resources of any known errors or changes. Coram will not be held responsible for any errors unless you have notified us of the relevant changes.

9.2 All service users are responsible for:

- Where relevant, ensuring that any information that they provide in connection with their access to services is accurate and up to date.
- Where relevant, informing their Coram key worker of any changes to information which they have provided, e.g. changes of address.
- Where relevant, informing their Coram key worker of any known errors or changes.

10. Related Policies

- Information Governance Framework
- Retention of Data Policy
- Open Information Policy
- Information Security Policy
- Confidentiality Policy
- Records Management Policy
- Privacy Policy

Appendix A

Application to make a subject access request under the Data Protection Act 1998

All data subjects including staff, volunteers, associates, students, and other users of Coram services or facilities have the right to access any personal data that is being kept about them. Any person who wishes to exercise this right should complete the form below and forward it to the Coram Data Protection Officer, together with a cheque for £10, made payable to Coram.

If you would like to view your HR file in person, please indicate this in Section 4. You will be entitled to receive a copy of the requested information within 40 days of the date that your identity is verified and payment is received. You will also receive an acknowledgement from us indicating the deadline when the request will be due.

1. Personal Details of Data Subject			
Surname:		First Name(s):	
Address:			
Postcode:			
Daytime telephone no.:			
Email address:			
2. Employment History of Data Subject (ex-employees only, to assist us in accessing your information)			
Service/Project employed within:			
Job Title:			
Dates Employed:			
Line Manager's Name:			
3. Details of information being requested (please include all relevant information to assist us in identifying the information you require)			

4. Means of access

Please indicate in relevant box:

☐ Collect copies from Coram ☐ Copies to be sent by recorded delivery ☐ Review file in office*

* Please confirm the dates/times that you are available to visit the Human Resources office:	

5. Identification

You are required to provide identification to the Data Protection Officer when collecting your documentation from the office.

If you are a current member of staff, your Coram ID card will be acceptable.

If you are not a current member of staff, you will need to provide one item from each of the two lists below:

1. Photographic ID e.g. passport, driving licence
2. Proof of address such as Council Tax bill, utility bill, bank or credit card statement from the last three months.

6. Declaration

By signing below you indicate that the information supplied on this form is true and accurate and that you are entitled to apply for access to the personal data detailed in this form under the Data Protection Act 1998. Coram may need to contact you for further identifying information before acceding to your request. You warrant that you are the data subject and will fully indemnify us for all losses, cost and expenses if you are not.

Signature:	Date:

Please return this form with a cheque for £10 made payable to Coram to:
Coram Data Protection Officer, 49 Mecklenburgh Square, London, WC1N 2QA

Appendix B

Amendments Summary

Date	Issue	Additions	Deletions	Amendments
January 2011	**3**			p.3 Named contact for data control issues changed to Carol Homden.
March 2011	**4**	p.3 Email address added for DPO.		
January 2012	**5**			p.3 Data Protection Registration expiry date updated.
January 2013	**6**			p.3 Data Protection Registration expiry date updated
October 2013	**7**			Name of DPO changed
February 2014	**8**	Section 3: Data controllers for Voice, CCLC and the Foundling Museum		DPO changed to Christine Kelly