Title:	**DATA PROTECTION**
Type:	**POLICY**
Group:	**DATA PROTECTION**
For:	**CHAILEY HERITAGE FOUNDATION**

Lead:	Jane Cope	**Role:**	Data Protection Officer
Support:	Tyrone da Silva	**Role:**	IT Services Manager

Agreed by:	Governor Finance Committee	**Signature:**	Signed on original
Date:	26th June 2017	**Name:**	Mike Atkinson
Agreed by:	Board of Governors	**Signature:**	Signed on original
Date:	10th July 2017	**Name:**	Dr Elizabeth Green

Review Frequency:	3 years or when specific regulations change
Next Review Process to Start:	Summer 2020
This document will remain valid during the review process	

LINKED DOCUMENTS:
Children's Homes Regulations and Quality Standards 2015 CQC Fundamental Standards Safeguarding Policy IT Acceptable Use Policy IT Acceptable Use Procedure All Policies, Procedures, Guidelines, Protocols for Chailey Heritage Foundation

VERSION CONTROL:			
Date	**Version No**	**New or reasons for revision**	**Agreed by**
June 2017	2.0	Reviewed and major updates made.	Governors

DATA PROTECTION POLICY

1. PURPOSE

1.1 Chailey Heritage Foundation (CHF) has a values system which upholds the importance of privacy for the individual whether it be a pupil, a young adult, a member of staff, a parent or member of the community, and this underpins its commitment to data protection.

1.2 As a Data Controller, CHF is required to maintain certain personal data about living individuals for the purposes of satisfying operational and legal obligations. The types of personal data that CHF may require include information about: current, past and prospective employees; CHF Trustees, Governors and donors; suppliers; young people and young adults who use CHF's services. This personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998. CHF has registered its use of personal data to the Information Commissioners Office as required under the Act.

1.3 The Chief Executive will appoint a Data Protection Officer for the Foundation. Responsibilities are listed in Appendix 3

2. EQUALITY IMPACT

2.1 This policy will ensure that confidential data about all stakeholders held securely and only shared internally where there is need and externally where there is a clear, legal requirement to do so.

2.2 At CHF the arrangements for protecting the privacy of clients and staff shall not prevent the sharing of data that needs to be shared and that damage that might result from not sharing information.

2.3 In particular requirements under Safeguarding regulations must be adhered to .

3. RESPONSIBILITIES

3.1 CHF fully endorses, and adheres to the eight principles of the Data Protection Act 1998. Employees and any others who obtain, handle, process, transport and store personal data for CHF must adhere to these principles.

3.2 The **eight principles** require that personal data shall:

3.2.1 Be processed fairly and lawfully and shall not be processed unless certain conditions are met;

3.2.2 Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;

3.2.3 Be adequate, relevant and not excessive for those purposes;

3.2.4 Be accurate and, where necessary, kept up-to-date;

3.2.5 Not be kept for longer than is necessary for that purpose;
3.2.6 Be processed in accordance with the data subject's rights;
3.2.7 Be kept secure from unauthorized or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organizational measures; and
3.2.8 Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation the processing of personal data.

3.3 CHF is responsible for ensuring its compliance with the Data Protection Act. All staff are responsible for the implementation of this Policy. All staff must be made aware of the principles of the Act and attend any necessary training. It is the responsibility of managers to remind staff of Data Protection requirements as appropriate and to ensure that staff have attended data protection training as required.

3.4 Any breach of this policy should be reported immediately to line management and the Data Protection Officer (currently the Director of Finance).

4. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

4.4 Data must be processed in line with data subjects' rights. Data subjects have a right to:
4.4.1 Request access to any data held about them by CHF.
4.4.2 Prevent the processing of their data for direct-marketing purposes.
4.4.3 Ask to have inaccurate data amended.
4.4.4 Prevent processing that is likely to cause damage or distress to themselves or anyone else.

4.5 Any correspondence concerning a data subject's rights received by a member of staff must be in writing and should be forwarded to the line manager or Data Protection Officer immediately.

4.6 A formal request from a data subject for information that is held about them must be made in writing. Any member of staff who receives a request relating to access to personal information (sometimes known as a 'Subject Access Request') should request that it be put in writing. The request should then be forwarded immediately to the Data Protection Officer. The request must be acknowledged and information provided within 40 calendar days.

4.7 Data sharing agreements must be held with third parties eg CCS.

5. THIRD PARTY INFORMATION

5.1 Much of the personal data CHF holds will contain information about, or from, third parties. By the nature of our service, our main third party is Chailey Clinical

Services and the personal information relates to the health of children and young adults.

5.2 Any information that relates to, and identifies, other individuals must not be released unless that other individual has consented or if it is reasonable in all the circumstances to comply with the request without their consent.

5.3 Third party information or data must not be released to anyone without the direct consent of that third party, eg Chailey Clinical Services. In some cases, it may be more appropriate for the person/organisation requesting information or data to make a direct approach to the third party.

6. DATA SECURITY

6.1 Appropriate security measures must be taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

6.2 The Data Protection Act requires procedures and technologies to be put in place to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with our procedures and policies, or if he puts in place adequate measures himself.

6.3 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

6.3.1 Confidentiality means that only people who are authorised to use the data can access it.

6.3.2 Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

6.3.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored securely on the central computer system and not on individual's PCs.

6.4 The level of security required will be dependent upon the sensitivity of the personal data and the risk of it being compromised. As a minimum, security procedures should include consideration of the following:

6.4.1 Entry controls. Any stranger seen in entry-controlled areas should be reported.

6.4.2 Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

6.4.3 Methods of disposal. Paper documents should be shredded. Digital media should be physically destroyed when no longer required.

6.4.4 Equipment. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

6.4.5 Encryption. Where it is necessary to transfer sensitive personal data by way of a portable device or via email, such information should be encrypted.

7. PROVIDING INFORMATION OVER THE TELEPHONE

7.1 Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information. In particular they should:

7.1.1 Check the caller's identity to make sure that information is only given to a person who is entitled to it.

7.1.2 Suggest that the caller put their request in writing if uncertain about the caller's identity or if their identity cannot be checked.

7.1.3 Refer to the line manager or Data Protection Officer for assistance. No-one should be bullied into disclosing personal information.

7.1.4 Where providing information to a third party, do so in accordance with the eight data protection principles.

8. ENSURING PROTECTION OF PERSONAL DATA - PRIVACY IMPACT ASSESSMENTS

8.1 A Privacy Impact Assessment (PIA) must be considered whenever there is a change to the way that data is processed, whenever new activities are performed, or at the start of any project where personal information may be processed. Guidance on conducting a PIA is available from the Data Protection Officer. Conducting a PIA ensures that any new risks are identified and suitable controls put in place to ensure the on-going protection of personal data.

9. ARRANGEMENTS FOR MONITORING AND EVALUATION

9.1 The Data Controller Officer will arrange for an annual audit report, indicating how CHF complies with each of the enforceable principles in the Data Protection Act 1998.

10. APPENDICES:

Appendix 1 - Confidentiality of Information
Appendix 2 – Risk Assessment for data breach

APPENDIX 1

CONFIDENTIALITY OF INFORMATION - TO BE SIGNED BY ALL USERS WITH ACCESS TO CHF DATA

Much of the work undertaken by personnel at Chailey Heritage Foundation, by staff at ALL levels, involves confidential material. It is the responsibility of all users to maintain the confidentiality of this information and not to reveal it to any person outside of Chailey Heritage Foundation unless this disclosure is required within a work context. In all cases, the express written permission of the individual and/or the parent or guardian or from the member of staff concerned should be obtained, before the release of such information.

All information whether received verbally or by written or computer based records are the property of Chailey Heritage Foundation and must be treated as such. No records or data should be removed from Chailey Heritage Foundation except in exceptional circumstances.

If, for any reason, any member of staff undertakes to complete work away from their normal work place (e.g. at home) the following guidelines must be adhered to:

1. No employee may take material or equipment from Chailey Heritage Foundation without the express consent and knowledge of the line manager/supervisor.
2. The employee must take every reasonable care that information is not disclosed to any third party.
3. Computers used away from the work place but linked to our servers must be encrypted and must not be left logged on to our server
4. Care must be taken not to leave laptops in places where they can be stolen, eg parked cars
5. Passwords must be kept secure and must not be divulged to other parties
6. All material (including removable storage) or equipment must be returned to Chailey Heritage Foundation within the agreed time scales.
7. It is the responsibility of all line managers/supervisors to ensure that all material or equipment is returned.

All staff are expected to respect and maintain confidentiality of any information acquired while at work. Staff will naturally take a pride in their work and wish to talk about Chailey Heritage Foundation. This should not result in the identification of an individual or result in the divulgence of information concerning their family or their circumstances.

If you are in doubt about any aspect of your work that may fall into this category, you should consult with your head of department.

****

I have read and understood the Confidentiality of Information notes pertaining to Chailey Heritage Foundation. I understand that if I disclose or use information other than in the course of my normal duties I am liable to disciplinary action.

Signed:	
Print Name:	
Date:	

APPENDIX 2

RISK ASSESSMENT NUMBER:	
DATA BREACH ON:	
DESCRIPTION OF INCIDENT:	
RISK:	
CONCLUSION DRAWN:	
FURTHER ACTION TAKEN:	
PREVENTATIVE MEASURES TAKEN TO PREVENT REOCCURRENCE:	
FORM COMPLETED BY:	
DATE:	
APPROVED BY DATA PROTECTION OFFICER:	
SIGNED:	
DATE:	