Royal Free Hospital Children's School
Data Protection and Security Policy
March 2021

1. Introduction and Scope

1.1 The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 are the laws governing the processing of personal data in the United Kingdom. They apply to anyone that uses or accesses personal data.

1.2 This policy sets out how RFHCS processes personal data and complies with the legislation referred to in section 1.1 and covers all processing of personal data whether in electronic or paper formats.

1.3 RFHCS is a Data Controller registered with the Information Commissioner's Office (ICO) Z4574236 and must comply with the regulations in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed. The school must be able to demonstrate compliance. Failure to comply exposes the school to civil claims and/or enforcement action from the ICO that may include financial penalties.

1.4 Staff, when processing personal data for school business, are acting on behalf of the Data Controller, and for avoidance of doubt, when this policy refers to actions the school shall take, it also means the staff involved with the processing of relevant personal data.

1.5 This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by the rules and policies made by the school. Any failures to follow this policy may result in disciplinary proceedings.

2. Personal Data

2.1 Personal data only includes information relating to natural persons who can be identified or who are identifiable, directly from the information in question, or who can be indirectly identified from that information in combination with other information (for example: name, address, date of birth, National Insurance number, bank account details etc.).

2.2 Personal data may also include special categories of personal data. This is information about racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, biometric data. Separate rules also apply in relation to information relating to criminal convictions.

2.3 RFHCS will only collect and process this information for specific purposes where allowed by the law (for example equal opportunities monitoring) or where it has asked and received consent to do so.

2.4 The school is required to adhere to the six Data Protection Principles specified in article 5.1 of the GDPR. The school is also required to maintain records that demonstrate this compliance by article 5.2 of the GDPR. This is achieved by this policy document, maintaining a record of processing activities in an Information Asset Register, and any further policies that are specific to those processing activities.

2.5 This policy deals with the Data Protection Principles in sections 4 through 9.

3. Data Protection Officer

3.1 The school is required by the legislation to appoint a Data Protection Officer (DPO). The Data Protection Officer is Andrew Maughan, Borough Solicitor for the London Borough of Camden. He can be contacted at schoolsdpo@camden.gov.uk or 0207 974 4365. The Data Protection Officer is supported by Data Protection Advisors that monitor these contact details and carry out business-as-usual tasks on his behalf.

3.2 The role of the Data Protection Officer helps the school to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

3.3 Should data subjects, e.g. pupils, parents, or staff, have concerns or enquiries regarding Data Protection, they should in the first instance discuss these with the school's leadership. But if this is not possible or not practical in the circumstances, they may contact the DPO directly.

4. Fair, lawful, and transparent.

4.1 The school commits to compliance with the first Data Protection Principle by handling Personal Data fairly:

4.1.1 The school will only process Personal Data in ways which would reasonably be expected of a school and will be honest and transparent about the reasons for any processing. Should there be any processing required which may be unexpected or unusual, school leadership in conjunction with the DPO will take steps to inform the subjects as far as reasonably possible under the circumstances. This may take the form of an extra Privacy Notice. (See Section 4.3 (Privacy Notices))

4.1.2 If there may be any adverse effects on data subjects due to processing the school will give consideration to these and be able to justify any such processing. See section 11 – Data Protection Impact Assessments.

4.2 The school commits to handle personal data lawfully by assessing the lawful basis for all significant processing activity. This will be maintained in the Information Asset Register, and where necessary, recording in a DPIA.

4.3 The school is committed to transparency and upholding the right of the data subject to be informed of how their data is being processed. This is normally done through providing a copy of, or a link to, the School's Privacy Notice

http://www.royalfree.camden.sch.uk/page/?title=GDPR+and+Information+Handling&pid=28.

Additional Privacy Information may be communicated with data subjects as required.

4.3.1 This Privacy Notice or additional information will be provided at the time the information is collected. Should the information be obtained from a third party, such as the Local Authority or Department of Education, the school will normally provide this information within 30 calendar days.

5. Purposes of processing

5.1 The school shall process data only for the purposes it was originally collected, or compatible purposes. The purposes will be communicated with the data subject in a Privacy Notice as per section 4.

5.2 Should a need arise to process data in an additional or different way to the purposes originally specified, the school's leadership shall consult the DPO regarding a Data Protection Impact Assessment. The new purposes must be found to be lawful and fair, and then communicated transparently as per section 4.

6. Data Minimisation

6.1 The school will not collect more data than it requires. For significant processing activities, the Information Asset Owners listed in the Information Asset Register will be responsible for ensuring that only the minimum information required for the specified purpose is held, and no more. Often this will involve reviewing forms that are used to collect data, and ensure that there are not fields collecting information that is no longer used.

6.2 For any other processing carried out on behalf of the school, the staff carrying out the processing will be responsible for compliance with this principle. In summary, staff should assess the need to collect personal data before doing so, and only collect personal data when necessary, and then only the minimum data required.

7. Data Accuracy

7.1 For significant processing activities, the Information Asset Owners listed in the Information Asset Register shall be responsible for ensuring accuracy of data. This will involve an assessment of the risks associated with the data being or becoming inaccurate and implementing an appropriate procedure for ensuring the data obtained is accurate and is kept accurate.

7.2 Individual staff remain responsible for keeping and maintaining their own accurate records for any other processing undertaken.

8. Retention and Destruction

8.1 Personal data shall be kept only for as long as it is required for the purpose it was collected for and no longer.

8.2 The school has a Retention and Destruction Policy to specify how long information is kept for. It also specifies how it is disposed of at the end of this period.

Once a recruitment (or other relevant) decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints. If, in very exceptional circumstances, it is considered necessary to keep Disclosure information for longer than six months, we will consult the DBS about this and will give full consideration to the data protection and human rights of the individual before doing so. Throughout this time, the usual conditions regarding the safe storage and strictly controlled access will prevail.

Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding. While awaiting destruction, Disclosure information will not be kept in any insecure receptacle (e.g. waste bin or confidential waste sack). We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, notwithstanding the above, we may keep a record of the date of issue of a Disclosure, the name of the subject,

the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

8.3 Each entry in the Information Asset Register shall have a corresponding entry in the Retention and Destruction Policy.

8.4 The Information Asset Owners are responsible for ensuring deletion/destruction is carried out in accordance with the Retention and Destruction Policy, and also for keeping the necessary records to show that data have been appropriately destroyed.

8.5 Other records (those not included in the Asset Register) may also be included in the Retention and Destruction Policy to assist with managing files. Staff will seek advice if uncertain about how long they should be keeping a record.

9. Information Security

9.1 For significant processing activities, the Information Asset Owners listed in the IAR shall be responsible for carrying out a risk assessment and ensuring security measures in place adequately reflect the risks associated with that processing. This is in addition to any basic requirements set out below.

9.2 **Digital Technology See E Safety Policy – Acceptable Use Policy**

9.3 **Paper and other hard copy data**

9.3.1 Staff must store data securely at all times and should never store data, even temporarily, where it may be at risk (e.g. staff must not take data to a pub or restaurant on the way home, or leave it in the back of a car overnight or when at the supermarket).

9.3.2 Paper based information should only be carried outside the organisation if absolutely necessary and only with the explicit approval of the Head Teacher or authorised deputy

9.3.3 This information should not be read or displayed on public transport, or in public spaces due to the risk of unauthorised disclosure.

9.3.4 Where it is absolutely necessary to keep confidential information at home (for example key emergency contact details or business continuity plans) as sanctioned by a manager with the necessary authority, these documents must be kept securely under lock and key. This means that such information should be stored in a private lockable cupboard or similarly secure space, and should be kept out of sight (e.g. not left on tables or in hallways where it would be visibly obvious to unauthorised persons, such as housemates, or intruders).

9.3.5 Paper based information should also be stored separately from high value items such as laptops wherever possible, and should not be kept together in a laptop bag.

9.3.6 Staff must ensure they know who to contact for security advice and guidance, including when working remotely, and how to contact them.

10. Automated processing and decision making

The school does not carry out any automated processing or decision making using personal data.

11. Individual Rights

11.1 Subject Access

11.1.1 Individuals ("Data Subjects") have the right to access their personal data. The person who the personal data is about is known as the data subject and the person who is making the request is known as the applicant. These can of course be the same person depending on the personal data sought. A common example of this relationship would be when a parent (applicant) is seeking personal information about their child (data subject).

11.1.2 To request access to personal data that the school holds about a Data Subject, a Subject Access Request (SAR) form can be completed and submitted to the School. The form is not a requirement as a valid request does not have to be in a specified format. But for convenience of record keeping the school requests that applicants use the form.

11.1.3 Parents may request information about their children. However, the legislation specifies that the rights over personal data rest with the subject of that data, providing that the subject has sufficient maturity and competency to understand their rights. There is no prescribed age specified in the legislation for this, but other parts of the legislation indicate that 13 is a reasonable starting point. This means that:

11.1.3.1 Pupils aged 13 and over [individual schools may wish to change this depending on their circumstances] may be informed when a request is made, and their right refuse to allow disclosure.

11.1.3.2 In the case of any child (including those under the age of 13) refusing to allow disclosure, an assessment must be made of their competency. If a child is assessed as competent then their control over their personal data for these purposes cannot be overridden by the wishes of the parents.

11.1.4 The school must take sufficient steps to be satisfied of the identity of the applicant and their right to the information. To these ends, the school may request any identification documents reasonably necessary to establish identity. These will normally include:

11.1.4.1 one piece of photographic identification, such as a valid passport, valid driving licence or a valid EU national identity card.

11.1.4.2 one piece of identification confirming address and dated within the last three months such as a utility bill, council tax statement or bank statement.

11.1.5 There is no fee for a Subject Access Request. Where a request is manifestly unreasonable or excessive then the school will opt to refuse the request rather than charge a fee as allowed by the legislation.

11.1.6 The school has one calendar month to respond to a subject access request. This may be extended in some circumstances which will be explained at the time they occur.

11.1.7 The details in this policy are a summary only. The school will manage Subject Access with due regard to the Information Commissioner's Office Subject Access Code of Practice, and where necessary, in consultation with the Data Protection Officer.

11.1.8 A separate right exists under the Education (Pupil Information) (England) Regulations 2005 (SI 2005/1437) for parents to view their child's Educational Record free of charge. However, a charge may be made for providing a copy of these documents.

11.2 Other individual rights

11.2.1 Further rights provided by the legislation and relevant to the processing carried out by the school are:

- Right to rectification
- Right to erasure (Right to be forgotten)
- Right to restrict processing

- Right to object to processing

11.2.2 The school will uphold these rights in accordance with the legislation. Individuals wishing to know more about these rights should be referred to the Information Commissioner's Office website. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

11.2.3 To exercise their rights data subjects should contact the School Business Manager

12. Closed Circuit Television (CCTV)

12.1 The school uses CCTV for the purposes of:

12.1.1 Monitoring entrance to the school and allowing office staff to observe visitors.

12.1.2 Security and crime prevention

12.2 CCTV is / is not recorded.

13. Information Asset Register

13.1 The school is required by Article 30 of the GDPR to keep a record of data processing activities. This is maintained in an Information Asset Register.

13.2 For each Asset listed in the register, there will be specified:

13.2.1 The purposes the information is used for.

13.2.2 The categories of data subjects (e.g. students, parents, staff)

13.2.3 The categories of personal data (e.g. contact details, educational records, employment records)

13.2.4 The retention period for that data, or link to the retention and destruction policy.

13.2.5 Details of any transfers to international organisations or third party countries.

13.2.6 Security measures protecting the data

13.2.7 The condition(s) under Article 6 and/or Article 9 of the GDPR that allow the processing

13.2.8 The lawful basis relied on for the processing

13.2.9 The details of any joint Data Controllers

13.2.10 The information necessary to demonstrate compliance with any of the other functions referred to in this policy. e.g. sections 4 through 9.

13.2.11 The Information Asset Owner (IAO)

13.3 The maintenance of this register will be overseen by the School Business Manager and the responsibility for ensuring each entry remains accurate and is regularly reviewed lies with the corresponding IAO.

14. Information Sharing with third parties / joint controllers / processors

14.1 The school shall only share data with third parties when the following conditions are met:

14.1.1 There is a contract in place with specifying how the third party will process data on behalf of the school.

14.1.1.1 All contractors are required to meet specified data security standards, and have adequate policies in place.

14.1.2 There is a written Information Sharing Agreement in place with another Data Controller such as the Local Authority or another school which describes the responsibilities of both parties.

14.1.3 An exemption applies which allows or requires the school to disclose data to that third party (for example, to assist with police investigations or by the order of the courts).

14.1.3.1 Police or other parties asking the school to disclose data for these purposes should contact us

14.1.4 Where other conditions set out in regulation 6 and/or regulation 9 of the GDPR apply and permit personal data to be shared. E.g. the subject has given consent.

14.2 The school does not store or transfer data outside of the European Union.

15. Data Breaches – See Model Camden Policy

16. Privacy by design and default, and Data Protection Impact Assessments (DPIA)

16.1 Whenever the school is implementing a new system or business practice that involves the processing of personal data, the school will observe privacy by design.

16.2 A DPIA is a risk based approach required by the GDPR to identify and manage high risk processing by identifying it and associated risks early.

16.3 All new projects or systems which involve a significant amount of personal data processing require a DPIA screening questionnaire to be completed by the project manager.

16.4 The screening questionnaire shall be submitted to the school's management and the DPO, who will advise on the risks and whether a full DPIA is required.

16.5 For those projects considered to be High Risk, or otherwise requiring a full DPIA, the project manager and the DPO will prepare the full DPIA for submission to the governing body for approval before the project is able to proceed.

16.6 The screening questionnaire, the full DPIA, and associated guidance about how to complete these is found [here]

17. Photography

17.1 The school uses photographs of individuals for the following purposes:

17.1.1 Security and access purposes (ID cards or passes)

17.1.2 To assist staff with the identification of pupils with allergies

17.1.3 Class photographs – records for posterity.

17.1.4 Our own publications – such as newsletters, our website, or the prospectus.

17.1.5 Providing photographs for other media to use in their publications.

17.2 Consent will be sought for the use of photographs at the start of the school year except where the use of photographs is considered essential to the operation of the school or the safety of pupils (sections 17.1.1 and/or 17.1.2)

17.2.1 Wherever practical, the school will ask for consent at the time they require the use of the image. In order to make management of publications practically possible, the school may rely on the blanket consent given, referred to in 17.2, for using the photographs where the use would be reasonable and expected by the subject.

17.2.2 Where the use would be considered exceptional, the school will seek specific consent from the subject as per section 20 below.

18. Telephone Call Recordings

18.1 The school does not record telephone calls that are made and Outgoing calls are not normally recorded.

19. Biometrics

19.1 The school does not use biometric data in any way.

20. Consent

20.1 In order to process personal data, the school relies primarily on the conditions provided by regulation 6(1)(c) (legal obligation) or 6(1)(e) (public task). The condition provided by 6(1)(a) (consent) will normally only be used when another does not apply.

20.2 When consent is used as the basis for processing, the school shall request consent and that request shall:

20.2.1 Be in writing.

20.2.2 Require a positive action to "opt in" or give consent.

20.2.3 Be clear and concise and where consent is being asked of a child; extra care shall be taken to phrase the consent in terms they are likely to understand.

20.2.4 As far as practicable in the circumstances, be specific and granular to avoid blanket consent or any other possible confusion.

20.2.5 Be provided alongside a Privacy Notice. (See section 4.3 of this policy)

20.2.6 Explain how to withdraw consent.

20.2.6.1 It will always be possible for consent to be withdrawn at any time after it has been given, although if the processing has already occurred it may not be possible to reverse that. e.g. If a publication is already printed and distributed, and a subject changes their mind about the use of a photograph, the school may only be able to stop the use of that photograph in future publications.

20.3 Processing shall not take place until the consent request has been completed and returned. The consequences of this will be explained in the request.

20.4 Consent from children

20.4.1 The rights provided by the legislation rest with the subject of the data. This means that where the data is about children, and where the child has sufficient maturity and understanding, the child may exercise their right to consent, or withdraw consent, as appropriate. There is no fixed age provided by the legislation, but as a starting point, children aged 13 years or older will be informed of consent requests and their associated rights.

20.5 The school will maintain sufficient records of consent to be able to demonstrate that consent has been given or withdrawn for any processing of personal data relying on consent until that processing has ceased.

21. Review

This policy will be reviewed annually by the Headteacher. This policy is subject to as required by developments in case law or guidance issued by the ICO or other official body. Changes may occur without advance notice.

Updated: March 2021

Date approved by governors: 18/3/21

Due for review: March 2022