Data Sharing Agreement

Name of Data Sharing Agreement:	
Between:	**Virgin Care Services Limited** "Virgin Care" and Schools in Lancashire "Partner Organisation"
Virgin Care Service:	Lancashire Healthy Young People and Families Service
Brief outline of agreement:	The agreement will facilitate the sharing of Class Lists and Health Assessment Questionnaires and the NCMP. This will also facilitate the sharing of personal identifiable data for the purposes of Direct Care.
Date of agreement:	April 2019
Next date of review:	April 2022 (unless any significant changes are required)

Version Control			
Date	**Status**	**Reason for update**	**Reviewed by**
25 March 19	Final	The service change to Virgin Care as the providers of the 0-19 Service	Alex Knox

Table of Contents

1. Introduction

1.1. This Data Sharing Agreement ('the agreement') is an overarching agreement to facilitate the exchange of data between the organisations party to it ('parties').

1.2. All organisations involved in providing services to the public have a legal responsibility to ensure that their use of all person identifiable data ('personal data') is lawful, properly controlled and that an individual's rights are respected.

1.3. The agreement provides a framework for safeguarding the processing of personal data, however it is incumbent on parties to recognise that any data shared must be justified on the merits of each case.

1.4. Adherence to this agreement does not provide any form of legal indemnity for any party from data protection legislation or any other law. It only serves to justify the data shared and to demonstrate that the parties have been mindful of and documented compliance with the relevant laws, nationally dictated organisational responsibilities and guidance.

1.5. The agreement is not intended to replace local policy but to support it and provide guidance where none already exists. It should also be read in conjunction with the staff guidelines in place within each organisation regarding the transfer or sharing of personal data.

1.6. The Caldicott Guardian or Senior Information Risk Owner (SIRO) **must** sign on behalf of each organisation. Where no such position exists, a Director or most senior person responsible for Data Protection requirements may act as signatory.

2. Scope

2.1. The aim of this agreement is to ensure that the data sharing is appropriately covered in a straightforward and transparent manner.

2.2. The agreement applies to all persons working in or for the parties organisations ('staff') e.g. employees, volunteers, contractors, students, those employed via agencies, etc. who have access to the personal data on the system.

2.3. The parties must ensure this agreement is disseminated, understood and acted upon by relevant staff, via training or other communicated means.

2.4. The parties must ensure that the specific department or team involved in the data sharing is clearly identified. Internal organisational access to shared data must be limited to those with a legitimate and approved need to see that data.

2.5. The agreement applies to all data processed under this agreement by the organisations, no matter in what format.

3. Definitions

3.1. **Data Protection Legislation:** The General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018 and the common law duty of confidence (confidentiality) all provide individuals with the right to privacy and confidentiality and the expectation that healthcare organisations will keep their data safe and secure.

3.2. **Controller:** A controller determines the purpose and means of processing personal data. Where engaging a processor, GDPR places further obligations to ensure contracts with processors comply with GDPR.

3.3. **Processor:** A processor is responsible for processing personal data on behalf of a controller. The GDPR places specific obligations on processors to maintain records of personal data and processing activities. Processors will also have legal liability if responsible for a breach.

3.4. **Personal data:** any data relating to an identifiable person who can be directly or indirectly identified in particular by a reference to an identifier. Pseudonymised data call fall within the scope of GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

3.5. **Special categories of personal data:** any data relating to an individuals' race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life or sexual orientation.

3.6. A glossary and list of abbreviations can be found in Appendix A.

4. Data Sharing Agreement detail

Party	
Party	Virgin Care Services Limited
Data Protection Designation	Controller
Party	Named School
Data Protection Designation	Controller

Purpose, objectives of the data sharing
Class Lists The purpose of the sharing of information detailed in this agreement is: the sharing of personal identifiable information between the Lancashire Healthy Young People and Families Service (LHYPFS) and the named School. The information is being shared to: 1. Ensure that LHYPFS know which children are attending which school. This will enable Virgin Care to provide the school aged health service to the local population of children. 2. To ensure that LHYPFS know which children have moved in and out of the area. This will enable LHYPFS to forward Child Health records to other School Nurse services and request information from other School Nurse services in a timely manner enabling effective communication to provide school aged health services and to safeguard and promote the welfare of children 3. Ensure robust liaison arrangements between the school and the LHYPFS 4. Ensure individual children and young people are cared for appropriately according to their needs in order to meet any safeguarding concerns i.e. sharing of domestic abuse notifications on a need to know basis

5. Ensure schools are aware of which children require packages of care that may impact on the child's school education or attendance (with parental consent).
6. To enable identification of children who are not receiving, or at risk of not receiving, a suitable education

In addition to the information sharing guidelines in this document, the LHYPFS will need the following in order to fulfil their role:

- An appropriate room in school for visiting health representatives to see children and their families privately and confidentially as required
- An appropriate, confidential and safe space for school drops ins where these are provided within high schools.
- Support with the provision of time and space for:
- NCMP sessions in reception and Year 6
- Completion of school health needs assessments in Year 6 or Year 9 (by paper or electronic methods)
- Timely liaison regarding new parents meetings.

<u>Health Assessment Questionnaire's</u>

To develop comprehensive school health information profiles that allows schools and health services to understand and respond to individual and population needs.

That data and information is collected and then collated in such a way to maintain data protection and confidentiality whilst facilitating:

- School Nurses being able to access the individual data in order to meet individual need
- Schools to have summarised school report of anonymised health needs
- The local authority to obtain population level data for identification and strategic planning

Objectives:

1. Additional health information is collected from Year 6 and Year 9 pupils as part of the on-line health questionnaire that pupils complete. Secure individual unique pupil number (UPN) codes are used.
2. The system allows school nurses to be able to access individual health questionnaire results and make early responses to need.
3. Consent processes should be utilised to ensure that children, young people and families are aware of the process and understand why health questionnaires are being collected
4. To ensure privacy notices explain the process of the health needs assessment and what information is being shared
5. The school and school nurse work together to offer this health needs assessment.
6. The school nurse explains to children and young people about the health needs questionnaires, prior to completion
7. IT Systems are in place to support any individual child or young person to complete the form as required if additional help is required.
8. To ensure schools, head teachers, and teachers understand the process and why the information is being collected

9. To ensure that any IT platform and/or other system facilitates the sharing of information and protects this information at different sharing levels. Also Data Protection and data storage are in adherence to local and national standards.
10. To ensure school nurses are able to obtain contact details from school, of pupils that require follow up or further support after completion of the questionnaire.
11. Contact details of the School Nurse are displayed in schools to enable children, young people or families to make any further enquiries.

Benefits of the data sharing

- Improving the educational and health outcomes for children and young people
- Identifying need, in order to formulate actions, and allocating resources accordingly
- Sharing information safely, appropriately and within legislation for the benefit of children and young people they serve

Data Privacy Impact Assessment

Processing is not likely to result in a high risk to the rights and freedoms of natural persons: the justification signed by the Data Protection Officer is attached as an appendix.

Lawful basis for processing the data

Personal data can be processed and shared providing the processing and sharing complies with the Data Protection Legislation.

Sharing for Direct Care Purposes - Where sharing is for the purpose of delivery of direct care or administration (waiting list management, performance against national targets, activity monitoring, local clinical audit, production of datasets to submit for commissioning purposes and national collections), GDPR Article 6(1)e and 9(2)(h) is the most appropriate lawful basis.

These conditions will also apply where an organisation participates in activities with a statutory basis, such as responding to a public health emergency.

- **Article 6(1)e** – 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority'.
- Where special categories personal data is being processed for purposes related to the commissioning and provision of health and social care services the condition is:
- **Article 9(2)(h)** – 'processing is necessary for the purposes of preventive or occupational medicine, for ... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services...'

GDPR Article 6(1)(e) and Article 9(2)(h) is the lawful basis	Yes

Sharing for Safeguarding Purposes - For the purposes of safeguarding children and

vulnerable adults, the Article 6(1)(e) and 9(2)(b) may apply. The Children Act 1989 (CA) establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm. The CA also requires local authorities 'to safeguard and promote the welfare of children within their area who are in need' and to request help from specified authorities including NHS organisation. These are required by the CA to comply '…with the request if it is compatible with their own statutory or other duties and obligations and does not unduly prejudice the discharge of any of their functions'. Under the Children Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being.	
• **Article 6(1)e** – 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority'. • Where special categories personal data is being processed for purposes related to the commissioning and provision of health and social care services the condition is: • **Article 9(2)(b)** – ''…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law...'	
GDPR Article 6(1)e and Article 9(2)(b) is the lawful basis	Yes

Explicit consent is available as a lawful basis for processing special categories of data but is not normally use consent as a legal basis in a healthcare setting.	
Consent is the lawful basis	No

Data items to be processed		
Data item	Justification	Lawful basis
Class Lists and lists of children who have moved in or out of the school. Referral from the School to the School Nurses. <u>Personal Data:</u> Forename Surname Date of birth Gender Address	To support the Direct Care of the patients.	Children's Act (2004) – Section 10 and 11. GDPR Article 6(1)(e) and Article 9(2)(h) is the lawful basis

Postcode Telephone number Ethnicity Mobile number School Year Email address Parent/carer contact details Parental/Carer email address School URN <u>Special Category Data:</u> Medical Condition, needs and medication taken in school.		
Health Assessment Questionnaire Information to be shared by School nurses to schools ➢ Anonymised data from the health needs questionnaire which will be fed back to the school, in report format generated from the Lancashire County Council web platform Information to be shared by schools with Virgin Care School Nurses: ➢ As per the Class list information above.	To support the Direct Care of the patients.	Children's Act (2004) – Section 10 and 11. GDPR Article 6(1)(e) and Article 9(2)(h) is the lawful basis

Data sharing	
Who will share the data	Virgin Care and the Named School
How will the data sharing be carried out	For both purposes, the pre-existing templates that are already in use by the service will continue. Class lists – information will be transferred via secure NHS email

	Health information will be via the healthy lifestyles questionnaire on-line platform. The named school will be responsible for providing the UPN codes and children's names, date of birth to school nurses in order for them to access the system.
Who in each organisation will have responsibility for overseeing the Processing	School Nursing Team and the Named School.
How is the data secured and who is responsible for ensuring security	Each organisation will be responsible for the information that they process.
Is any data to be transferred outside the EEA	No
What record will be kept of what has been shared with whom	All completed health questionnaires will be transferred and stored within the child's individual health record.

Data Quality Detail	
How will data quality be managed; What is the process for ensuring omissions, errors, etc are corrected	Each organisation will be responsible to ensure that the data quality of the information is regular reviewed for accuracy.
Who will carry out the auditing	The School Nursing service and the named school.
Who is responsible for corrections	The School Nursing service and the named school.
What is the escalation procedure for problems	Any problems will be escalated to the appropriate lead for review.

Privacy Notice	
Who will advise data subjects about the processing carried out as a result of the data sharing covered by this agreement	School Nurses and the named School.
How will this be communicated	Verbally.
If you are processing any personal data about children, what have you done to ensure that your privacy notice is accessible to them	Privacy notices will be available on the Virgin Care Website, and individual paper leaflets.
Where joint controllership applies, has this been made clear in the	Virgin Care and the Named School will be joint data controllers and this will be clearly documented on the

privacy notice	Children's Privacy Notice.

Individuals' Rights	
Has a contact point for data subjects been indicated in the privacy notice	Details relating to the information will be documented in each organisation's privacy notice.
What is the process to keep the other party up-to-date about amendment, erasure or restriction of use of data shared under this agreement	Each organisation can be contacted directly should they wish to exercise any of their rights. If discussion is required then both organisations will arrange this discussion and where necessary link in with both Information Governance Teams.

Records Management Detail	
Is the data to be processed in paper	Yes this may be recorded and processed on paper in respect of the existing templates that are in place. The information must be transferred securely.
If yes, who will hold the paper data	Each organisation will be responsible for holding the records.
If yes, how will the paper data be stored	The organisation must be held securely in locked filing cabinets and access is only on a need to know basis.
How will the paper data be returned or destroyed	Disposal of confidential information in paper or digital format must be carried out in line with each organisations policy which must be in compliance with the NHS Digital Disposal of Confidential Data Guidance.

Shared system	
What is the name of the system(s)	N/A
Access control detail	N/A
What is required prior to a User being given access	N/A
Who will sign off the access to be given	N/A
Department and/or person who will give the User access to the data	N/A
How will access be given	N/A

Name of the person maintaining the list of Users and informing when a User no longer requires access	N/A
What is the procedure for terminating User access	N/A
Department and/or person responsible for terminating access	N/A
How will monitoring access to the data take place	N/A
Who will carry out the monitoring	N/A
What is the escalation procedure for problems relating to access to the data	N/A

Retention Periods	
How long will the data be retained for	All data, whether held on paper or in electronic format must be stored and disposed of in line with each partner organisation's retention and disposal schedule. Retention periods should be informed by the Records Management Code of Practice published on 20 July 2016 by the Information Governance Alliance (IGA).
Disposal of data	The disposal of confidential data in paper or digital format will be carried out in line with each organisation's policy which must comply with the NHS Digital Disposal of Confidential Data Guidance. This should include provision for notification of such deletion/destruction.

Management of the Agreement	
Who will keep signed copies of the agreement	The Head of Information Governance or person responsible for Data Protection at each Party will retain copies of the Agreement
Review of the agreement	The agreement will be reviewed annually for effectiveness unless the parties become, or are made, aware of reasons for an earlier review.
Who will undertake the review of the agreement and agree any changes	The Caldicott Guardian or person responsible for Data Protection and/or the Head of Information Governance at each Party will undertake the review and agree any changes

Who will pay for associated costs of any review	Costs will be borne equally by the parties
Can this agreement be shared as part of the publication scheme of the organisation (if relevant)	Yes
How will the agreement be terminated	This agreement will be terminated by agreement of the parties or by non-compliance

5. Key contacts

Key Contacts Virgin Care	
Senior Information Risk Owner (SIRO)	Lynne Shamwana
Virgin Care Caldicott Guardian	Peter Taylor
Head of Information Governance	Sarah Murray - Information.Governance@virgincare.co.uk
Local IG Lead	Alex Knox
Deputy Caldicott Guardian	To be confirmed
Information Asset Owner	Dawn Matthews-Smith
Sponsor	
Clinical Systems Manager (where relevant)	Sarah Smallwood

Key Contacts [Named School]	
Senior Information Risk Owner (SIRO)	
Caldicott Guardian	
Head of Information Governance	
Information Asset Owner (where relevant)	
Other contact(s) eg. IT contact,	

service/department contact, etc.	

6. General Obligations of all parties to this agreement

If there are particular tasks required of a party these can be documented in the tables above.

6.1. This agreement must be agreed by all parties to be in force.

6.2. The parties agree to be responsible for ensuring full compliance of all staff within their organisation to the terms and conditions of this agreement.

6.3. All parties in this agreement will comply with the following general obligations:

General Obligations	
ICO	Be registered with the UK information Commissioner to carry out data processing activities and keep up to date its registration with the Information Commissioner
IG Toolkit	Each party shall Maintain Level 2 in the requirements of the Data Security and Protection Toolkit (DSPT) relevant to their Processor type, to include: • Cyber Essentials • IG training by all staff accessing personal data to be up-to-date
Data Controller arrangements	Be responsible for the data they hold and process (once safely received) from the other party as data controller of that information
Data sharing oversight	Have appointed and named a responsible officer who will ensure the protection of personal data, e.g. Caldicott Guardian or senior manager responsible for data protection
Access to the data	Access to data by any user will be managed by agreed controls. Once a user is authenticated the user should only be able to access the records and data that they need for legitimate reasons.
Legal Compliance	Comply with its obligations under data protection legislation, policies and standards and under the common law duty of confidentiality
Lawfulness, fairness and transparency	Comply with 'The right to be informed', and ensure that details of any new processing/sharing will provided to the data subjects and be accurate, transparent and informative, and suitable for the intended audience
Purpose limitation	The data will only be processed by staff in order for them to perform their duties for the purposes identified and not processed for any other purposes. The core purpose is the provision of health and social care

	services, further processing of the data, such as managing and planning services, cannot be undertaken without the approval of all partners.
Data minimisation	Process only data which is adequate, relevant and limited to what is necessary
Accuracy	Take all reasonable steps to ensure data processed is correct. All parties are responsible for informing any source partner of any accuracy issues they identify within the data shared. Any data quality issues that may significantly affect the care of an individual will be reported to relevant partners immediately (i.e. any issue that may either delay provision of care or risk the effectiveness of care). Issues that are not critical, such as a potential misinterpretation of data should be reported so that issues can be assessed and addressed.
Storage limitation	Will not keep personal data for longer than it is need for the purposes identified
Integrity and confidentiality	Agree to treat the data received under the terms of this agreement as confidential and safeguard it accordingly and respect the privacy of individuals at all stages of processing. All parties, whether they are providing or just viewing data, are responsible for implementing appropriate technical and organisational measures to ensure the security of the data within any shared system.
Accountability	Be responsible for, and be able to demonstrate, compliance with the data protection principles.
Overseas Processing	Before information can be processed outside of the UK all parties must be informed of this intent with sufficient notice in writing. Information will not be processed outside of the European Economic Area without the appropriate safeguards being in place.
Complaints, queries and objections	Notify the other parties to this agreement of any complaint received from any person about the sharing of data under this agreement or any correspondence from the Information Commissioner or other regulator regarding the sharing of data under this agreement. Assist each other in responding to requests made under the Freedom of Information Act 2000 or Environmental Information Regulations 2004 in relation to the data shared under this agreement to ensure a co-ordinated and consistent response, unless an exemption under the Act applies. Where information is held jointly, it is the responsibility of the organisation receiving the request to ensure they request promptly all relevant information from the other parties. Where one party receives a request meant for the other, such requests will be sent to the other party immediately and safe receipt confirmed.
Breach	Information breaches will be the responsibility of the party in which the breach occurred. All breaches should be assessed in line with the 'Guide to Notification of Data Security and Protection Incidents' (https://www.dsptoolkit.nhs.uk/Help/29). This provides a common tool for

	scoring of incidents, noting when an incident should be reported to the Information Commissioner's Office and affected individuals. Where a party identifies a reportable breach, it should inform any other parties within 24 hours. A breach that is not classed as reportable will be managed by the partner identified as responsible and will engage other parties as required.
Use of third parties (processors)	The parties to this agreement will not instruct further processing of the shared data by any third parties without the consent in writing of the partner organisations.

7. Indemnity

7.1. Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other [reasonable] professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the breach of the Data Protection Legislation by the indemnifying party, its employees or agents, provided that the indemnified party gives to the indemnifier prompt notice of such claim, full information about the circumstances giving rise to it, reasonable assistance in dealing with the claim and sole authority to manage, defend and/or settle it.

8. Review of agreement

8.1. The data sharing and this agreement will be reviewed by a suitably qualified individual or committee/group within each organisations, at a minimum annually, and on an ad hoc basis as and when required to ensure the agreement remains fit for purpose and that the data sharing is continuing to effectively achieve its objectives. This agreement will remain in force irrespective of whether the agreement has been officially reviewed until a notice of termination is served.

9. Termination and variation

9.1. Any partner organisation may leave this agreement by giving thirty calendar (30) days' notice in writing to Virgin Care Services Limited.

9.2. Any proposed changes to the parties involved in this agreement, to the purposes of the data sharing, the nature or type of data shared or manner in which the data is to be processed and any other suggested changes to the terms of this agreement must be notified immediately to the relevant Information Compliance/Governance leads so that the impact of the proposed changes can be assessed.

9.3. No variation of the agreement shall be effective unless the agreement is amended and it is signed by all parties.

9.4. Each party will abide by the provisions of this agreement until such time as the processing of the personal data ceases. However the terms of this agreement remain binding in respect of any data shared and retained throughout its lifecycle, irrespective of whether the party remains a current signatory to this agreement.

9.5. On termination of this agreement any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this agreement which existed at or before the date of termination, shall not be affected.

10. Dispute resolution

10.1. In the event of a dispute arising under this agreement, authorised representatives of the parties will discuss and meet as appropriate to try to resolve the dispute within seven calendar (7) days of being requested in writing by any party to do so. If the dispute remains unsolved, it will then be referred to a senior manager from each of the parties who will use all reasonable endeavours to resolve the dispute within a further fourteen calendar (14) days.

10.2. In the event of failure to resolve the dispute through the steps set out above the parties agree to attempt to settle it by mediation.

11. Signatures

Signed for and on behalf of:

Organisation: Virgin Care Services Limited	
Name: Dawn Matthews-Smith	
Position: Managing Director – Lancashire 0-19 Service	
DPA Registration No. Z2823541	Date of expiry/re-registration: 23/08/2019
Signature:	
Date:	

Signed for and on behalf of:

Organisation: INSERT SCHOOL DETAILS	
Name: XXXX	
Position: Caldicott Guardian	
DPA Registration No. XXXX	Date of expiry/re-registration: XXXX
Signature:	
Date:	

12. Appendix A – Glossary and abbreviations

Caldicott Guardian	A senior person responsible for protecting the confidentiality of patient and service-user data and enabling appropriate data-sharing.
Consent forms	Consent forms are forms that are used to obtain the permission of the data subject for their personal data to be used for a particular purpose. A consent form can be used at the point of collection (as part of the collection text) or later, if the particular purpose was not explicitly mentioned when the data was collected. Specific conditions must be met when using consent as a legal basis. These should be documented within the DPIA.
Data	"Data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.
Data Controller	A Data Controller determines the purposes and means of processing personal data. Each legal entity within Virgin Care will be a Controller or a Processor as identified in the health care contract.
Data Controller: Joint	Joint controllers are two or more controllers that jointly determine the purposes and means of processing. No matter what the arrangement is between the joint controllers, the data subject may exercise his or her rights in respect of and against each of the controllers. Data Controllers in Common is not a concept under new data protection legislation.
Data Processing	Data Processing means any manual or automated actions in relation to the data. Actions includes collection, recording, storage, alteration, retrieval, use, disclosure by transmission, blocking, erasure and destruction. There must be a lawful basis for processing personal and special category data and any processing must comply with the data protection principles.
Data Processor	A Data Processor is responsible for processing personal data on behalf of a controller. Under new data protection legislation a data processor has a number of obligations. Data processors as well as data controllers are liable to data subjects for breaches. Each legal entity within Virgin Care will be a Controller or a Processor as identified in the health care contract.
Data Subject	A Data Subject is the individual who is either the direct subject of the personal data, or can be identified from it. Data subjects have the right to compensation from a data controller or data processor.
Data: Personal data	Information which has been gathered by the controller or processor relating to a living individual which identifies them.

	Personal data can include pseudonymised data depending on how difficult it is to attribute the pseudonym to a particular individual.
Data: Special Category data	Data concerning health is classed as special category data and requires additional conditions and safeguards. The inclusion of genetic and biometric data as sensitive personal data is new and will need to be reflected in policy and contracts.
Data: Anonymised	Data protection legislation does not apply to data that is fully anonymised in such a way that individuals cannot be identified.
Data: Pseudonymised	Pseudonymised data will be treated as personal data because individuals can potentially be identified, albeit via a key.
Deceased individual	The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased service user. These individuals are defined under the Act as, 'the service user's personal representative and any person who may have a claim arising out of the service user's death'. A personal representative is the executor or administrator of the deceased person's estate.
Health and/or Care Record	A record which consists of data relating to the physical or mental health and/or social care of an individual
Privacy Notice	Privacy notices are to inform the person from whom personal data is being collected, the data subject, how data is going to be processed. Specific information must be provide to the data subject.
Publication schemes (Freedom of Information Act)	The Freedom of Information Act places a duty on public authorities to adopt and maintain a publication scheme that must be approved by the Information Commissioner.
Senior Information Risk Owner (SIRO)	The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy and who acts as advocate for information risk.
Subject Access Request for living individual	A subject access request (SAR) is a request received from an individual asking to provide them with copies of the data held about them. Individuals have the right to access data held about them under the Data Protection Act 1998 (DPA).
Third Party	A person or organisation other than the data subject or Virgin Care.
DPA	Data Protection Act. The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018. It sits alongside the General Data Protection Regulation (GDPR), and tailors how the GDPR applies in the UK - for example by providing exemptions.
DPIA	Data Protection Impact Assessment. The DPIA is one of the specific processes mandated by the GDPR. Organisations must carry out a DPIA where a planned or existing processing operation –"is likely to result in a high risk to the rights and freedoms of individuals".
DPO	Data Protection Officer. The GDPR makes it a requirement that organisations appoint a DPO in some circumstances.

DSPT	Data Security and Protection Toolkit (replaces the IG Toolkit from April 2018)
GDPR	The General Data Protection Regulation. GDPR came into force on May 25, 2018, and is designed to modernise laws that protect the personal data of individuals. It also boosts the rights of individuals and gives them more control over their data.
ICO	The Information Commissioner's Office is a UK independent supervisory authority. It enforces and oversees the Data Protection legislation and the Freedom of Information Act 2000.
IG	Information Governance.
IGA	The Information Governance Alliance; the authoritative source of advice and guidance about the rules on using and sharing data in health and care.

13. Appendix B – Data Privacy Impact Assessment

(or statement by DPO justifying why a DPIA is not required)