

Coventry and Warwickshire Partnership Trust – Immunisations in Schools

Between:

Warwickshire County Council,
and

School Immunisation and Vaccination Service: Coventry and
Warwickshire Partnership Trust (CWPT)

**Nasal flu will be offered to children in reception and years
1, 2, 3, & 4**

**Information from Warwickshire Local Authority's
Admissions Service is requested for children who have:**

- **Been offered a place in reception class in Sept 17**
- **Been offered a place in Year 3 in Sept 17** (*Y2 transfer from
Infant schools*)

**Information from May 2017 school census is requested for
children who are currently in:**

- **Reception, Y1, 2 and 3**

**And from October 2017 school census, children who are
currently in:**

- **Y8 - girls only**
- **Y9 - boys and girls**

Information Sharing Protocol – May 2017 v0.2

Document Control

Title	Coventry and Warwickshire Partnership Trust – Immunisations and vaccinations for children attending Warwickshire’s state-funded schools and academies
Purpose	The purpose for sharing this information is to enable the national immunisations and vaccinations schedule to be delivered to eligible pupils by Coventry and Warwickshire Partnership Trust (CWPT). These eligible pupils for academic year 2017/18 are in Reception, Y1, 2, 3 and 4 for nasal flu, Y8 girls for HPV, Y9 girls for 2 nd dose HPV and Y9 boys and girls for Teenage booster (Td/IPV& and Meningitis ACWY)
Review Date	April 2018
Author	Insight Service, Performance Business Unit, Resources Group
When and what data will be shared	<p>To facilitate this information sharing in a timely way and to enable CWPT to have the pupil data prior to the start of each academic year for planning purposes, Warwickshire County Council will supply:</p> <p>Pupil level data from the Admissions Service for children starting in reception in September 2017. This will also include children due to start in Year 3 transferring from Infant schools</p> <p>Pupil level data from the May 2017 School Census covering current year groups; reception, Y1, 2 and 3</p> <p>Pupil level data from the October 2017 census for Y8 girls and Y9 boys & girls</p> <p>Data supplied will be; School DfE number, School Name, Year Group, Pupil surname, Pupil Forename, Date of Birth, Gender, Full address including postcode.</p> <p>Data will be supplied to CWPT in July 2017 (from May census and Admissions) and December 2017 (from October census) for the relevant year groups each year</p>
Caveats	<p>The Summer School Census takes place annually on the third Thursday in May and again in October. It is a snap-shot in time and reports the data held in a school’s management information system on Census day.</p> <p>Therefore it will only reflect the situation at that point in time and will be subject to change if, for example, a child moves school or address, any new children start at a school or other circumstances change.</p> <p>Every effort is made by the school and Local Authority to ensure this data is as accurate as possible on Census day but please be aware that data supplied to CWPT may change prior to the immunisation and vaccination programme starting in the new academic year. The same caveats apply to the Admissions’ new intake and Y3 transfer data.</p>
Who the data will be shared with	<p>Ann Curzons. Service Manager Immunisation and Vaccination Service Integrated Children’s Services</p> <p>ann.curzons@nhs.net or ann.curzons@covwarkpt.nhs.uk</p>

Information Sharing Protocol – May 2017 v0.2

Revision Date	Reviser	Version	Description of Revision
15 th May 2017	Ann Curzons/Naomi Wills	0.1	Changes to the year groups data as a result of a change in the programme
23 rd May 2017	Julie Robottom	0.2	Update to the agreement to reflect new data being collected (Reception intake) from another team (Admissions) at the Local Authority.

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
Andrew Morrall	Information Manager, Warwickshire County Council	andrewmorrall@warwickshire.gov.uk
Naomi Willis	Information Governance Manager Coventry & Warwickshire Partnership Trust	Naomi.wills@covwarkpt.nhs.uk

Information Sharing Protocol – May 2017 v0.2

Contents

1	Introduction	5
2	Purpose	5
3	Scope	5
4	Parties	5
5	Basis for Sharing	6
6	Information to be Shared	7
7	Privacy Impact Assessment (PIA) and Information Risk Assessment	7
8	Transfer and Security of information	7
9	Ensuring Data Quality	8
10	Information Use	8
11	Information Retention and Deletion	9
12	Training and awareness	9
13	Access to Information	9
14	Roles and responsibilities	9
15	Review	10
16	Breaches of Security	10
17	Signatures	10
Appendix 1	Contact List	12
Appendix 2	Conditions for Processing Personal Data	13
Appendix 3	Information Sharing Standard and Related Guidance	14
Appendix 4	Glossary	15

Information Sharing Protocol – May 2017 v0.2

1 Introduction

- 1.1 This Information Sharing Protocol has been drawn up to set out the core information sharing principles which have been agreed by the signatory organisations.
- 1.2 This protocol has been formulated to facilitate the exchange of information to identify eligible children for national immunisations and vaccinations between the protocol signatories. It is, however, incumbent on all partners to recognise that any information shared must be justified on the merits of the protocol. The balance, between an individual's Human Rights and the need to disclose information, must be assessed to ensure the information shared between agencies is proportionate to the purpose. Anyone in doubt should consult their organisation's Data Protection or Information Sharing officer before proceeding.

2 Purpose

- 2.1 The purpose of this protocol is to provide an appropriate framework to facilitate the sharing of information between the organisations signed up to this protocol, to provide the national immunisation and vaccinations to children. In order to meet this objective it is necessary for partners to share selected information.
- 2.2 The purpose of the information sharing is to enable Coventry and Warwickshire Partnership Trust to have a full list of all children offered reception places for academic year 2017/18 and the current reception, Y1, 2 and 3 children, and from the October 2017 census, Y8 girls & Y9 boys & girls that are eligible for the national immunisation and vaccinations, to enable them to issue consent forms and letters for the immunisations and monitor those provided.
- 2.3 In order to achieve this in a timely way for the start of each academic year, Warwickshire County Council will supply data about pupils who have been offered a place in reception in academic year 2017/18 and those in year groups reception, Y1, 2 and 3 from the May 2017 (Summer) School Census. and girls in Y8 & boys and girls in Y9 from the October 2017 (Autumn) School Census
- 2.4 The information covered in this Protocol can only be used for the purpose for which it was collected. If any of the Partners to the Protocol want to change the purpose, all Partners need to agree to the change. If a partner to the Protocol wants any of the data for further statistical purposes, personal information should be anonymised.

3 Scope

- 3.1 This Protocol is intended to formalise:
 - The organisational requirements to share data about children and young people by the organisational signatories of this document.
 - To enable Coventry and Warwickshire Partnership Trust to receive a list of Warwickshire pupils in specific year groups that Warwickshire County Council have records for so that they can match this data with the health data for NHS numbers and can check medical history. It is then used to issue consent forms and the information letters to each child via their school.
- 3.2 This protocol is not intended to cover information sharing between an agency/organisation and any other third parties (e.g. member of the public/journalist).

4 Parties

- 4.1 This protocol is between the parties listed in **Appendix 1**, from the following organisations:

Information Sharing Protocol – May 2017 v0.2

- Warwickshire County Council
- Coventry and Warwickshire Partnership Trust

- 4.2 If a new party **joins** the protocol, a new version of the information sharing protocol will be issued as soon as possible and circulated to **all** participating parties.
- 4.3 If a party **leaves** the protocol, a new version of the information sharing protocol will be issued as soon as possible to **all** participating parties. Parties must refer to section 13 regarding retention and deletion of information that has been shared.

5 Basis for Sharing

- 5.1 The signatories to this Protocol are able to share information because of the following legal powers:

Children Act 2004,

Section 10, places a duty on each Authority's Children's Service to work with relevant partners to improve the wellbeing of children in relation to: Physical and mental health, and emotional well-being

- Protection from harm and neglect
- Education, training and recreation
- Making a positive contribution to society
- Social and economic well-being

Strategic health authorities and NHS Trusts are named as relevant partners and *Section 11* of the act places a duty on key people with the relevant authorities to ensure their functions are carried out with regard to 'safeguard and promote the welfare of children.

Children Act 1989,

Section 17, places a duty on a local authority to safeguard and promote the welfare of children within their area who are in need; and so far as is consistent with that duty, to promote the upbringing of such children by their families, by providing a range and level of services appropriate to those children's needs.

Education Act 2002,

Section 175 places a duty on a local authority that they shall make arrangements for ensuring that their functions as a local education authority are exercised with a view to safeguarding and promoting the welfare of children.

The National Health Service Act 2006,

Section 82, places a duty on NHS bodies and Local Authorities to co-operate with one another in order to secure and advance the health and welfare of the people of England and Wales.

For copies of the Acts go to www.legislation.gov.uk but bear in mind that amendments made subsequent to the act may not show up on these copies.

Information Sharing Protocol – May 2017 v0.2

- 5.2 The relevant Data Protection Act Schedule 2 condition for sharing this personal data under this protocol is schedule 2 para 5(b) - the processing is necessary for the exercise of any functions conferred on any person by or under any enactment.
- 5.3 Any information shared and the processes used to share such information will be compliant with the relevant Human Rights legislation.

6 Information to be Shared

6.1 The information shared under this ISP comprises:

Information Set	Organisation(s) providing the information	Organisation(s) receiving the information	Retention Period	Specific instructions regarding use of this information set (eg. method of disclosure)
Personal Data about the child First Name, Surname, DOB, Gender, Full address, School attending.	Warwickshire County Council: Insight Service	Coventry and Warwickshire Partnership Trust: School Immunisation and Vaccination Service	3 Months	That it is only used for the purposes described in this protocol and sent via a secure method.

- 6.2 If there is a need to share additional information on a one-off-basis, the parties concerned should consider whether the sharing is necessary to the protocol and document their considerations/findings, including any additional consents sought (and if not sought, an explanation as to why).
- 6.3 If additional information is required on a repeated basis over and above what is defined in this protocol, to enable the protocol to achieve its aims, the lead officers should agree an addition to the sharing protocol, ensuring that the new information meets the same legislative or consent basis as the original. This addition should be added to the protocol and all parties should sign up to it.

7 Information Risk Assessment

7.1 All parties have achieved a satisfactory compliance against the current HSCIC Information Governance Toolkit requirements, which covers information governance and security.

As the information to be shared contains personal s it will need to leave the secure environment of one to reach the secure environment of the other.

7.2 In order to mitigate this risk the Insight Service will send the information via secure e-mail using Egress security protection or the Government Secure Email service from warwickshire.gscx.gov.uk to nhs.net.

8 Transfer and Security of information

8.1 Signatory parties have Information policies and procedures in place to set out the minimum standards of security they require. Where parties do not have a specific policy in place the following principles should be followed

- unauthorised staff and other individuals are prevented from gaining access to personal data;

Information Sharing Protocol – May 2017 v0.2

- computer systems containing personal data are password protected and passwords are not disclosed to others;
- users lock their screen, or sign off their computers when not in use;
- physical records (paper files, discs, printouts etc) are stored in secure locations and only accessed by those who need to use them
- use appropriate methods to transfer personal data by secure/encrypted email eg. PSN email (GCSx)
- operate a Clear Desk Policy and do not leave confidential information on public display
- all new software has been authorised and disks are virus-checked prior to loading onto your computer
- use secure methods for the disposal of electronic and physical information

8.2 The information sharing in this protocol requires the following specific security requirements:

- **All information shared must be sent via e-mail using Egress security protection or the Government Secure Email service from warwickshire.gscx.gov.uk to nhs.net.**

8.3 The following methods are not to be used to share information under this protocol:

- **Any other transfer method, other than those mentioned above.**

8.4 Information that is shared should be labelled with the name of its originator, so that obligations around withdrawal of consent, updating to maintain accurate records and reporting any breaches etc can be fulfilled.

9 Ensuring Data Quality

9.1 Everyone sharing data under this protocol is responsible for the quality of the data they are sharing.

9.2 Before sharing data, officers will check that the information being shared is accurate and up to date to the best of their knowledge. If sensitive personal data is being shared which could harm the individual if it was inaccurate, then particular care must be taken.

9.3 Regular data quality spot-checks of information shared (eg. through dip-sampling) should be undertaken to verify the accuracy of the data being shared.

9.4 Where a 'dataset' is being shared (i.e. structured data), it will be accompanied by a table providing definitions of the data fields.

9.5 If personal data has been held for longer than 3 months an updated version must be obtained before any action is taken.

9.6 If a complaint is received about the accuracy of personal data which affects datasets shared with partners in this protocol, an updated replacement dataset will be communicated to the partners. The partners will replace the out of date data with the revised data.

10 Information Use

10.1 Parties to this protocol undertake that information shared under the protocol will only be used for the specific purpose for which it was shared, in line with this protocol. It must not be shared for any other purpose outside of this protocol.

10.2 The recipient will not release the information to any third party without obtaining the express written authority of the party who provided the information.

Information Sharing Protocol – May 2017 v0.2

11 Information Retention and Deletion

- 11.1 The retention period for the information shared is 3 months from the date of transfer to ensure the information used is up to date.
- 11.2 Secure methods of disposal will be utilised to destroy information at the end of its retention period.
- 11.3 If a party leaves the protocol, decisions must be taken and followed through on what happens to:
 - The information that has already been shared with the signatories by the departing organisation
 - The information that has already been shared with the departing organisation by the other signatories

12 Training and awareness

- 12.1 All organisations will be expected to promote staff awareness of this protocol and its contents.
- 12.2 All staff processing information shared under this protocol are expected to be suitably trained to understand the legal requirements of information sharing and their responsibilities under the Data Protection Act and related legislation. This is an obligation on each organisation and responsibility cannot be assigned to another organisation.

13 Access to Information

- 13.1 Data Subjects have a right of access to personal data held about them, subject to any relevant exemptions which may apply.
- 13.2 Any Subject Access Requests (SARs) received by organisations which include data shared under this protocol will be processed by the receiving organisation and may be disclosed to the individual without the need to obtain the provider's consent. It is best practice to seek a view on disclosure from the providing organisation, but this is not a legal requirement.
- 13.3 The receiving organisation will consult the providing organisation for a view on disclosure if they have any concerns, or in the following circumstances:
 - an exemption from disclosure may apply to the information supplied (eg. legal professional privilege; prevention and detection of crime;)
 - the providing organisation has previously stated that the information supplied is subject to an exemption from disclosure
 - the receiving organisation is not sure whether an exemption from disclosure applies
 - a health practitioner has supplied the information

14 Roles and responsibilities

- 14.1 All partners to this agreement must appoint a Point of Contact and ensure that this Point of Contact remains up-to-date. [Appendix 1](#) details the current Point of Contacts for each organisation.
- 14.2 The Point of Contact within each organisation will be the first port of call for questions about the information sharing protocol. If there is a problem such as a potential information security breach, relevant point of contacts must be contacted.
- 14.3 It is the responsibility of everyone sharing, accessing and using the information shared to take appropriate decisions about the sharing and use of the information. This includes holding and transferring the information securely, and in accordance with the standards set

Information Sharing Protocol – May 2017 v0.2

out in the overall sharing standard and this agreement. Any person who is still unclear on requirements to fulfil this responsibility should in the first instance read the standard and this protocol, and then, if necessary, contact their organisation's Point of Contact detailed in [appendix 1](#).

- 14.4 Only appropriate and properly authorised persons will have access to the information specified in this Agreement. If in doubt, a person intending to share or access information should contact their Point of Contact detailed in [appendix 1](#).

15 Review

- 15.1 This Information Sharing Protocol will be reviewed 12 months after its launch and thereafter no less frequently than every 12 months. The person responsible for initiating this process is: Commissioning Intelligence Manager, Insight Service, Warwickshire County Council
- 15.2 If a significant change takes place which means that the protocol becomes an unreliable reference point, then the protocol will be updated as needed and a new version circulated to all organisations involved in the information sharing initiative to replace the old.
- 15.3 If the lead person departs their role, an alternative lead must be nominated as soon as possible.

16 Breaches of Security

- 16.1 All parties will have in place appropriate measures to investigate and manage incidents that compromise, or potentially compromise, personal data.
- 16.2 The party making the discovery will without delay advise the other party.
- 16.3 If there is a security breach in which information received from another party under this ISP is compromised, the party making the discovery will notify the both party responsible for the breach (if not themselves) and the party who provided the information (if known) without delay via the lead contacts listed in [appendix 1](#).
- 16.4 The party responsible for the breach will be the lead in managing the response and co-ordinating any mitigating actions that may be required. This will include:
- inform the information provider of the details and liaise with them, and other parties in the ISP as appropriate, to ensure an appropriate and co-ordinated response is made;
 - consider whether the breach requires a (temporary) suspension of any further information sharing under this ISP
 - take steps to investigate the cause;
 - take disciplinary action against the person(s) responsible (if appropriate);
 - take appropriate steps to avoid a repetition;
 - undertake a risk assessment (in conjunction with the information provider if appropriate);
 - record on the HSCIC SRI if an appropriate level;
 - consider notifying the Information Commissioner's Office (ICO)
 - post-incident review with ISP parties to identify improvements which can be made to processes to avoid a recurrence of the breach
- 16.5 Parties providing information under the protocol may also review whether the breach impacts of further information sharing under this ISP.
- 16.6 The party who was responsible for the breach will accept total liability for a breach of this Information Sharing Protocol should legal proceedings be served in relation to the breach.

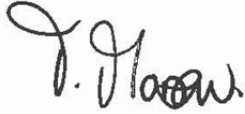
Information Sharing Protocol – May 2017 v0.2

17 Signatures

- 17.1 By signing this agreement, all signatories accept and understand their responsibilities for its execution and commit to abide by them. They also agree to ensure that staff are adequately trained so that requests for information and the process of sharing itself are sufficient to meet the purpose of this agreement.

Signed on behalf of **Warwickshire County Council**:

Name: Tricia Morrison

Signature: 

Rank/ Position:
Head of Performance & Interim Head of ICT Services (WCC SIRO)

Date: 23/05/2017

Signed on behalf of **Coventry and Warwickshire Partnership Trust**:

Signature: 

Name: Gale Hart

Rank/ Position: Director of Finance, Performance & Information / Senior Information Risk Owner (SIRO)

Date: 23/05/2017

Information Sharing Protocol – May 2017 v0.2

Appendix 1 Contact List

Organisation	Department	Named Point of Contact	Email
Warwickshire County Council	Insight Service, Performance Business Unit, Resources Group	Julie Robottom	Julie Robottom, Commissioning Intelligence Manager: julierobottom@warwickshire.gov.uk insight@warwickshire.gov.uk
Warwickshire County Council	Information Governance	Andrew Morrall	Andrew Morrall, Corporate Information Manager: andrewmorrall@warwickshire.gov.uk informationmanagement@warwickshire.gov.uk
Coventry and Warwickshire Partnership Trust	Head of Information Governance	Naomi Wills	Naomi.wills@covwarkpt.nhs.uk

Information Sharing Protocol – May 2017 v0.2

Appendix 2 Conditions for Processing Personal Data

Schedule 2 – Conditions for processing personal data
<ul style="list-style-type: none">• Consent of the individual
<ul style="list-style-type: none">• Necessary for a contract with the individual or with a view to entering a contract
<ul style="list-style-type: none">• Necessary for a legal obligation that applies to you (other than a contract obligation)
<ul style="list-style-type: none">• Necessary to protect the vital interests of the individual (ie. life and death of an individual)
<ul style="list-style-type: none">• Necessary for administration of Justice, or Statutory obligation(s), or function of Government Department(s); functions of a public nature in the public interest (inc. Public Bodies)
<ul style="list-style-type: none">• Necessary for the legitimate interests of the organisation or of a third party receiving the information, except where there is unwarranted prejudice to the legitimate interests of the individual

Schedule 3 – Conditions for processing sensitive personal data
<ul style="list-style-type: none">• Explicit consent of the individual
<ul style="list-style-type: none">• Necessary to comply with employment law
<ul style="list-style-type: none">• Necessary to protect the vital interests of the individual or other person
<ul style="list-style-type: none">• Carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. NB extra limitations apply to this condition
<ul style="list-style-type: none">• Made public by actions taken by the individual
<ul style="list-style-type: none">• Necessary for legal proceedings, obtaining legal advice, or establishing, exercising, or defending legal rights
<ul style="list-style-type: none">• Necessary for administering justice, or exercising statutory or governmental functions
<ul style="list-style-type: none">• Necessary for medical purposes and undertaken by a health professional or someone subject to equivalent duty of confidentiality
<ul style="list-style-type: none">• Necessary for monitoring equality of opportunity and carried out with appropriate safeguards for individuals' rights
<ul style="list-style-type: none">• Conditions contained in the Data Protection (Processing of Sensitive Personal Data) Order 2000 (SI 417/2000) – typically these conditions are substantially in the public interest and which must necessarily be carried out without the explicit consent of the individual eg. preventing or detecting crime and protecting the public against malpractice or maladministration

Information Sharing Protocol – May 2017 v0.2

Appendix 3 Information Sharing Standard and Related Guidance

Information Sharing Charter for Warwickshire:

<http://www.warwickshire.gov.uk/sharinginformation>

ICO Data Sharing Code of Practice:

http://www.ico.org.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx

ICO Data Sharing Checklist:

http://www.ico.org.uk/for_organisations/guidance_index/~/_media/documents/library/Data_Protection/Practical_application/data_sharing_checklists.ashx

Appendix 4 Glossary

Anonymised information	Information from which no individual can be identified. Please see the ICO Anonymisation Code for best practice.
Assessment notice	This gives the Information Commissioner certain powers to assess compliance with the Data Protection Act.
Caldicott Guardian	A senior health or social care employee who has a strategic role for the management of patient/client information, including agreeing and reviewing protocols governing the protection, use and disclosure of patient information.
Data Controller	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Processing	Obtaining, recording, holding, organising, adapting, retrieving, consulting, disclosing, aligning, blocking, erasing or destroying the data. Processing effectively means doing anything with data.
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Data Protection Act 1998 (DPA)	The main UK legislation which governs the handling and protection of information relating to living people.
Data Sharing	The disclosure of data from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. This can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for any of a range of purposes.
Data Sharing Protocols / Agreements	See Information Sharing Protocols / Agreements: http://www.warwickshire.gov.uk/sharinginformation
Data Subject	An individual who is the subject of personal data.
Fair Processing Notice	Unless an exemption applies, the data subjects must be given certain information about the processing of their personal data, at the point of collection. The key elements of this are the identity of the data controller, the purposes of the processing and anything else necessary to guarantee fairness (this may include disclosures, how long their data will be retained). Also called a Privacy Notice.
Information Sharing Protocols / Agreements	Set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. Also called Data Sharing Protocols/Agreements
Interoperability	In relation to electronic systems or software, the ability to exchange and make use of information.
Notification	The Information Commissioner's Office maintains a public register of data controllers. Each register entry includes the name and address of the data controller and details about the types of personal data they process. Notification is the process by which a data controller's details are added to the register.
Personal Data	Data which relate to a living individual who can be identified – <ul style="list-style-type: none">• from those data, or• from those data and other information which is in the possession of, or is likely to come into the possession of,

NOT PROTECTIVELY MARKED

the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Impact Assessment (PIA)

A comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Privacy Notice

Please see: <http://www.warwickshire.gov.uk/schoolprivacynotices>

Processing

Any operation performed on personal data, including collection, use, disclosure, deletion.

Protective Marking

Practice of marking on documents and files the level of sensitivity of the information they contain, so that they may be handled accordingly. Usually makes use of an agreed set of categories.

Pseudonymisation

The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.

Sensitive Personal Data

Personal Data consisting of information as to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- whether he is a member of a trade union
- physical or mental health or condition
- sexual life
- the commission, or alleged commission, of any offence, and related proceedings

Subject Access Request (SAR)

An individual's right under the Data Protection Act, to request a copy of the information which is held about them

Third Parties

In relation to personal data, third party means any person other than the Data Subject, the Data Controller (including employees), or any Data Processors (including employees)