Arbour House School

Information and Data Governance, Protection and Management Policy

Date of Issue	Feb 2023
First issue date	May 2018
Version number and previous validation date	5
Next review date	Feb 2024
Governor policy owner	Bettina Jeppesen
Signed off by	Arbour House School Governing Body
Distributed to	Internal/ External

Policy Content

Contracts and review information

Introduction

The Data Controller (DC) and Data Protection Lead (DPL)

Responsibility of the School

Responsibility of Staff

Responsibilities of Parents/Guardians

Rights to access information – Subject Access Requests (SAR)

Freedom of information request (FOI)

Data Breaches

Data Retention

Reporting Policy Incidents

Monitoring and Evaluation

Appendix A – Role of Data Controller

Appendix B – Role of Data Protection Lead

Appendix C – Privacy Notice for Students

Appendix D – Privacy Notice for Employees

Appendix E – Data Asset Audit and Data Asset Audit Document - example

Appendix F– Staff Privacy Impact Assessment form

Appendix G – Process for dealing with subject access requests

- Subject access request record

Appendix H – Process for dealing with Freedom of Information (FoI) Fol requests

-Freedom of Information request record

Appendix I – Data Breach record

Policy Review Record

Contacts and review information

The overarching **Data Controller** (DC) for Arbour House is the Potens Regional Director Bettina Jeppesen.

The School **Data Protection Lead** (DPL) is Julie Perks, Headteacher

Introduction

Arbour House School needs to use information about pupils, staff and other users to allow us to fulfil our duties, and to provide other services with data that we have a legal, statutory or contractual right to process.

The school will comply with the data protection principles which are set out in the General Data Protection Regulations 2018 and other laws.

The Data Controller and Data Protection Lead

The Data Controller for has the overarching responsibility to ensure processes and controls of data are in place which will ensure that the collation, accessibility, storage and transferring of information is completed in line with the Data Protection principles.

Details of the responsibilities of the Data Controller are described in **Appendix A**.

Day to day matters will be dealt with by the Data Protection Lead (DPL) whose responsibilities are described in **Appendix B.**

Responsibilities of Arbour House School

Arbour House is committed to respect and protect the confidentiality of sensitive information relating to staff, pupils, parents and governors. To ensure this the school will:

- Register with the Information Commissioners Office (ICO) as part of Potens.
- Keep an up to date Data Asset Audit (DAA) which list all known uses of personal data in the school. This can be found in **Appendix E.**
- Inform individuals about their rights regarding data protection through the Privacy Statements for Students **Appendix C** and Privacy Statement for Employees **Appendix D**.
- Verify that systems are in place to manage personal data and confidential information will be examined to ensure they meet the data protection regulations.
- Monitor regularly its data protection and information security processes and change practices where necessary.
- Ensure that all data obtained and held has been obtained fairly and lawfully.
- Provide training to ensure all staff are knowledgeable about their rights and responsibilities.

Responsibilities of Staff

All staff are responsible for ensuring that any personal information they provide to the school is accurate and up to date.

Staff are responsible for ensuring that any personal data they use in the process of carrying out their duties/role:

- Is shielded from view of others during use.
- Is kept securely locked when not in use.
- Is stored on a secure **password protected local hard or network drive**
- Where for specific reasons, the school has approved use of removable storage such as laptop, tablet or USB memory stick these must be password protected and encrypted. The storage here should be temporary only.
- Personal identifiable information should not be used unless it is absolutely necessary and there is no alternative.
- Is not disclosed to any unauthorised third party.
- Is assessed and approved by the Senior Leadership Team or the DC with advice from the DPO (see privacy impact assessment form – Appendix D), if used within an app, web service or other application.

The unauthorised deviation or disclosure of the above may be viewed and dealt with as a disciplinary matter.

Responsibilities of Parents/Guardians

Arbour House School will inform the parents/guardians of its pupils of the importance to maintain up to date personal data. This will include an annual request for updating the Emergency Information Form.

Arbour House School will also seek permissions regarding matters of non-statutory use of personal data such as the use of images and names in publicity materials on induction or when required. The returns of these permissions will be recorded and maintained in the individual student files and communicated to staff appropriately.

Rights to Access Information - Subject Access Requests (SAR)

All individuals about whom the school holds personal data have the rights to:

1. Obtain from the school confirmation if and how personal data concerning him/her or their child is being processed. Where this is the case, have a copy of the personal data and the following information:

- The purpose of the processing.
- The third parties that the data will be shared with.
- The period for which the personal data will be stored.
- The existence of the right to request the school to correct, erase or restrict processing of personal data if the data can be proved to be incorrectly held.
- The right to lodge a complaint with a supervisory authority.
- Any available information as the source of the personal data held, where this was not collected from the individual/data subject.

2. If exemptions are placed on any data above because of safeguarding or other issues, the existence of this data will be declared.

Any person who wishes to access information should make a **subject access request** in writing and submit it to the Head teacher or the chairman of the Governing Body. The process for dealing with these requests is outlined in **Appendix G.** Arbour House School will deal with requests for access to personal information as promptly as possible and in accordance with advice from the ICO and other professional agencies.

Freedom of information requests

Arbour House has a process for dealing with Freedom of Information requests which is laid out in **Appendix H.**

Freedom of information requests can be made by any member of the public about processes, policies and other non-personal information about Arbour House School. These requests will be dealt with ensuring the rights of individuals (within the Data Processing Regulations) not to be identified are respected whilst maintaining legal responsibilities within the Freedom of Information Act.

Data Breaches

Arbour House, with reference to GDPR, recognises person-identifiable confidential information as:

- Data subject name, address, full postcode and date of birth.
- NHS number, URN and any notes, records and information about their education, medical
- Any pictures, photographs, images, videos or audio recordings.
- Anything else that may allow the data subject directly or indirectly to be identified, for example a rare illness, diagnosis, drug treatment or statistical analysis.

The school will inform the DC of any Data Breach identified or suspected. The DC will advise on any actions to be taken. Data breaches will be recorded, detailing the facts relating to the potential personal data breach, its potential effects and remedial action taken as outlined in **Appendix I**.

The individual whose data may have been breached, will be informed of this and in the case of a high risk to the rights, protection and freedoms of the person(s) involved, the School will without undue delay, but no later than 72hours subsequently, also make a referral to the Information Commissioners Office as required.

Data Retention

Under the Data Protection Principles, Arbour House School has a responsibility to keep data only for as long as we need to do so.

The school will follow the advice of the Information Records Management Society (IRMS) using their records management toolkit for schools (https://irms.org.uk/page/SchoolsToolkit) regarding the length of time that schools should keep any data.

The destruction of paper documents will be carried out via cross-cut shredder either by the school or by a third party commercial company. Any data held on any electronic devices will be deleted in line with policy. Records will be kept of the data destroyed and/or a certificate of destruction will be issued by a third party.

Reporting Policy Incidents

Any individual who considers that this policy has not been followed in respect of personal data should raise this matter with the Head Teacher or the Data Controller.

Appendix A– *Role of Data Controller (DC)*

Purpose

The Data Controller (DC) is responsible for monitoring compliance with current data protection law and has knowledge, support and authority to do so effectively. The DC will oversee and verify the school's data protection processes and advise the school on best practices.

Responsibilities

- Advise the school about their obligations under current data protection regulations
- Support the DPL in developing a joint understanding of the school's processing operations, information systems, data security processes, needs and administrative rules and procedures.
- Support the DPL in developing a joint understanding of the schools processing operations, information systems, data security processes and needs and administrative rules and procedures.
- Assist in cooperation with the DPL with the monitoring of the school's compliance with data protection law by:
    - Collecting information to identify data processing activities
    - Analysing and checking the compliance of data processing activities
    - Informing, advising and issuing recommendations to the school.
    - Ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate
- Advise on and assist the school with carrying out data protection impact assessments if necessary.
- Act as a contact point for ICO, assisting and consulting it where necessary including:
    - Helping the ICO to access documents and information.
    - Seeking advice on data protection issues.
- Act as a contact point for individuals whose data is processed such as staff, pupils and parents, including:
    - Responding with support from the DPL to subject access requests.
    - Responding with support from the DPL to other requests regarding individuals' rights over their data and how it is used.
- Take a risk based approach to data protection, including:
- Prioritising the higher-risk area of data protection and focusing mostly on these and uphold confidentiality as appropriate and in line with data protection law, in carrying out all duties of the role.
- Assist the DPL in maintaining a record of the school's data processing activities.
- Work with external stakeholders, such as suppliers or members of the community on data protection issues.
- Work with the DPL in fostering a culture of data protection throughout the school.
- Work closely with other departments and services to ensure GDPR compliances such as HR, IT and security.
- Work with the Senior Leadership Team to ensure GDPR compliance.

***Appendix B**– Role of Data Protection Lead (DPL)*

Responsibilities

- Verify that the school has registered with the ICO.
- Support the DC in advising the school about their obligations under current Data Protection regulations.
- Support the DC in developing and understanding of the school's processing operations, information systems, data security processes, needs and administrative rules and procedures.
- Assist in cooperation with the DC with the monitoring of the school's compliance with the data protection law by:
    - Collecting information to identify data processing activities.
    - Analysing and checking the compliance of data processing activities.
    - Informing, advising and issuing recommendations to the School.
    - Ensuring they have current and detailed information in data protection issues and changes to the law, attending relevant training as appropriate.
- Assist the DC in making sure that the school's policies are followed through:
    - Assigning responsibilities to individuals.
    - Awareness raising activities.
    - Co-ordinating staff training.
    - Conducting internal data protection audits.
- Act as a contact point for the DC in supporting individuals, whose data is processed, by:
    - Responding to subject access requests.
    - Responding to other requests regarding individual's rights 'over their data and how it is used.
- Assist the DC in maintaining a record of the school's data processing activities providing this on a yearly basis to the Board of Governors.
- Assist the DC in working with external stakeholders such as suppliers or members of the community on data protection issues.
- Working with the DC in fostering a culture of data protection throughout the school.
- Working with the Senior Leadership Team to ensure GDPR compliance.
- Assist with any additional tasks necessary to keep the school compliant with data protection law and be successful in the role.

Tasks associated with the above responsibilities should include:

- Act as the point of contact with the DC.
- Advising on procedures and forms to allow the Data Protection Policy to be adhered to.
- Provide advice on other associated policies and documents.
- Provide materials and advice in completing a Data Asset Audit and assist in its completion if necessary.
- Assist the DC with the annual Data Asset Audit.
- Use the training materials provided to assist the staff in keeping up to date with Data Protection issues.

Appendix C – *Privacy Notice for Students*

Privacy Notice for Students

General Data Protection Regulations 2018 (GDPR)

Arbour House is required by law to tell you about your rights and our obligations regarding our collecting and processing any of your personal information, which you or your parent/guardian might provide to us or we may collect during the time we provide educational services. We have a range of policies and procedures to ensure that any personal information we have about you is only kept when we have a right to hold it or with your specific active consent. We will always hold your personal data secure and confidential in line with the law. We have listed the relevant documents in a later section and can make any available for you to review.

We collect and process personal information about you where it is relevant to your education. We do this to fulfil our role as School/Educational Provider.

Due to the nature of our work as a school the information we collect is often of sensitive nature and may include personal characteristics, local authority record information, health information and some other types of information.

What personal information we collect about you

As a school, we must collect some basic personal information about our students, including date of birth, address, medical history and diagnosis. These personal details are essential for the school to operate. The information is contained in individual student files (manual and electronic), all of which are subject to strict security and authorised access policies. Personal information that becomes inactive, e.g. from initial enquiries and referrals are also kept securely for as long as it is needed, before being safely disposed of.

How we collect information

We collect information from referral documents, through assessment from you and your parents/guardian and any other person who may otherwise support you.

We will also obtain information from previous educational establishment, the local authority, your GP and/or other health related practitioners involved with you.

All personal information obtained to will always be treated in line with our explicit consent, data protection and confidentiality policies.

What we do with personal information

All personal information obtained about our students is used only for the purpose of enabling Arbour House School to provide an educational service which meets all regulatory standards and requirements. It will not be disclosed or shared for any other purpose.

How we keep your information safe

We have a range of policies that enable us to comply with all data protection requirements. Our organisational Information and Data Governance, Protection and Management Policy which contains information in relation to Data Protection including personal data, information Governance under the GDPR, access to records and information sharing with other agencies.

With whom we might share information

We only share the personal information of students, employees and others with their consent on a "need to know" basis, observing strict protocols in doing so. Most information sharing of students information is with other professionals and agencies involved with their education, health and wellbeing.

The only exceptions to this general rule would be where we are required by law to provide information, e.g. to help with a criminal investigation. Even when seeking to notify the local authority of a safeguarding matter or the relevant Regulatory Body of an incident that requires us to notify you, and we would assure ourselves that the information we provide is treated in confidence.

Where we provide information for statistical purposes, the information is aggregated and provided anonymously so that there is no privacy risk involved in its use.

How your personal information can be accessed

There are procedures in place to enable students or their parents/ guardians whose personal information we hold and might process in some way, to have access to that information on request. The right to access includes both the information and any uses which we might have made of the information. A subject access request can be made by contacting the schools Data Protection Lead.

You have a right to ask us to correct any inaccuracies in the information we hold about you. If any of the information we have recorded about you is not correct or is out of date please inform the Data Protection Lead at Arbour House who will either amend the information or add a note to show that you/your parent or guardian disagree.

How long we keep information

Arbour House will follow strict protocols and regulations which are in place. These determine how long schools must keep students information.

How we keep our privacy policies up to date

We have specific staff appointed to control and process personal information within the school and the wider organisation. These individuals have been delegated to assess continuously potential privacy risks and to carry out at least annually, comprehensive reviews of our data protection policies, procedures and protocols.

If you have any concerns about how we manage your/your child's personal information, please contact the Data Protection Lead the first instance.

You can also contact the Arbour House School Data Controller: Bettina Jeppesen, Regional Director Bettina.Jeppesen@potens-uk.com

If you have any further concerns about how we handle your information, you have a right to complain to the Information Commissioner's Office (ICO) who regulate compliance with data protection legislation: ico.org.uk/

Signed by/ On Behalf of (please delete as appropriate) Student:

Date:

……. ……

Signed Print Name

Representative's Role where applicable: ……..

Privacy Notice for Employees and Volunteers

General Data Protection Regulation (GDPR)

How your information will be used

1. As your employer, Potens needs to keep and process information about you for ordinary employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left. This includes how and where the data is stored. This also includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Company and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

2. We may sometimes need to process your data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes or reporting potential crimes. We will never process your data where legitimate business interests are overridden by your own interests unless you have given us consent to do so.

3. Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees.

4. The sort of information we hold includes
    - your application form and references
    - your contract of employment and any amendments to it
    - correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary
    - information needed for payroll, benefits and expenses purposes
    - contact and emergency contact details
    - records of holiday, sickness and other absence
    - records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records

5. You will, of course, inevitably be referred to in many company documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the company. You should refer to the Information and Data Governance, Protection and Management Policy.

6. We will keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your

ability to do your job and whether any adjustments to your job might be appropriate in order to support you. We will also need this data to administer and manage sick pay.

7. Where we process special categories of information relating to such areas as your racial or ethnic origin or biometric data, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency. Please note that Potens does not routinely ask for any biometric data.

   Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

8. In addition, we may monitor computer and telephone use, as detailed in our IT Policy. We also keep records of your hours of work by way of our time recording system via Caresys (or other rota system where relevant) or your submissions of Statement of Hours.

9. Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to our external pension schemes.

10 Information on the periods of time your personal data will be stored for is available as an appendix to the Potens Information and Data Governance, Protection and Management Policy (Appendix D: Retention, Archiving and Destruction Schedule).

How we will store your Data

11. As a direct result of your employment with Potens, we are required to process data about you. The data required is detailed above and has been provided by you or relevant third parties. All of this data is collected, processed and retained by Potens in line with the regulations set out in the General Data Protection Regulations (GDPR) and The Data Protection Act 2018 (DPA).

12. The storage of such data will be done in a secure electronic format and held on the Potens HR system (SelectHR) as this is the basis for the employee HR data file.

13. SelectHR is an Access Group product and was subject to a Data Protection Impact Assessment listing the aims, objectives and purpose of the system for Potens. To ensure that access to data is permitted to only relevant personnel and for the security of data, SelectHR has multiple levels of security which limits who can see the data and only permits access to the data which is relevant to their role within Potens. Each employee within Potens has an individual log in to the HR system, relevant permissions are assigned via the individual log in and only data that is relevant for the individual and their role will be available to view.

14. The Access Group policies regarding data protection and system and service provision security are available on request from payroll@potens-uk.com.

15. The SelectHR system is in use for all employees of Potens and it is Potens policy and intention to hold, store and process information about you electronically using SelectHR for the purposes of processing your HR and payroll records required during the course of your employment.

16. SelectHR and other relevant HR and payroll systems are used by Potens as the governance for the storage and processing of HR and payroll data relating to your employment. If, or where, you have exercised your right to refuse or withdraw consent to the use of relevant personal data about you, including the storage of electronic copies of documents on SelectHR, this may affect Potens' ability to hold and process your data for the purposes for which it is intended. In these circumstances, this may have an impact on your employment with Potens and will need to be discussed separately with your manager.

Your rights

17. Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request access to and correction or deletion of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

18. If you have provided explicit consent for the processing of certain aspects of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

19. You have the right to lodge a complaint to the Information Commissioners' Office if you believe that we have not complied with the requirements of the General Data Protection Regulation or the Data Protection Act 2018 with regard to your personal data.

Identity and contact details of controller and data protection officer

20. Potens as a Company is the controller and processor of data for the purposes of the Data Protection Act and the General Data Protection Regulations.

21. If you have any concerns on how your data is processed you can contact the Data Controller for Arbour House Bettina Jeppesen, Regional Director bettina.jeppesen@Potens-uk.com or you can write using the address of Potens Head Office, 68 Grange Road West, CH41 4DB

Please sign below to acknowledge receipt of this Privacy Notice and return one copy to your manager. The other copy is for your retention.

If you have any concerns about how the organisation handle your personal information, please contact Potens' Data Controller in the first instance.

If however you have any further concerns about how we handle your information, you have a right to complain to the Information Commissioner's Office (ICO) who regulate compliance with data protection legislation: ico.org.uk/

Signed: …… Date: …….

Appendix E *– Data Asset Audit* ***Example***

Arbour House will document the personal data it stores.
This document will be a dynamic document and be the responsibility of the DPL. It will be updated using the privacy impact assessment forms completed by staff.

This document can be in any format but should contain information about the type of data held why it is held and who it is shared with as well as any anticipated risks.

Description of Service	Type of data	Reason to hold data	Where is it stored	Is data shared with anyone	Risks
Contact details spreadsheet	Personal and sensitive data	Statutory Duties Education Act	Server – on the o Drive and hardcopy on the office	DfE LA	Inappropriate viewing,
E learning	Potential sensitive data on learning and performance	Learning Tool	Cloud? Contract with Potens	Head office	Lost passwords, inappropriate viewing

Appendix F *– Staff Privacy Impact Assessment Form*

Before the use of any new service that uses personal data, staff should fill in a privacy impact assessment form.

The Head Teacher and/or the DPL, with advice from the DC, will then approve the use and the information to be placed on the Data Asset Audit.

Privacy Impact Assessment (PIA) form for:

Data protection Principles:

- Processing to be lawful and fair.
- Purposes of processing be specified, explicit and legitimate.
- Adequate, relevant and not excessive.
- Accurate and kept up to date.
- Kept for no longer than is necessary.
- Processed in a secure manner.

This Privacy Impact Assessment form needs to be completed because:

- The use involves the collection of new information about individuals.
- The use compels individuals to provide information about themselves.
- The information about individuals will be disclosed to organisations or people who have not previously had routine access to the information.
- We are using information about individuals for a purpose it is currently not used for, or in a way it is not currently used?
- We are using new technology that might be perceived as being privacy intrusive? For example the use of biometrics or facial recognition.
- The information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records or other information that people would consider to be private.
- The use requires you to contact individuals in ways that the may feel intrusive.

Appendix F – Staff Privacy Impact Assessment Form

Describe the Service:			
Describe the data collected and the possible uses of the data:			
List of Data held	Collection of data		
	Possible uses		
Identify the privacy related risks and possible solutions:			
Privacy Issue	Risk to individual	DPA risks	Possible solution
1.			
2.			
3.			
4.			
5.			
Sign off and notes:			
Comments on risks:			
Processes that must be in place:			
Contact point for future privacy concerns: DPO: DPL: Date completed:			

Appendix G *– Process for dealing with Subject Access Requests*

On receiving a Subject Access Request or request for change or deletion of data, the DC or Arbour House will:

- Inform the DPL in the school (and the head teacher if necessary).
- Record the details of the request, updating this record where necessary (see next page).
- Reply to the requestor confirming the receipt of the request asking for clarity if there is confusion about which data is required.
- Contact the DC if clarity on the request is needed or procedure is needed.
- Identify the people responsible for gathering the necessary data.
- Gather the data indicating a deadline.
- Examine the data for redactions making sure there is no bleeding of data.
- Ask the requestor for an address and time for delivery.

The whole process should take no longer than 30 calendar days, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Please note the time for processing a request for and Educational Record is 15 days.

The Subject Access Requests are held here: Data Security Folder in the Office.

Appendix G- ***Subject Access Request Record***

Name of data subject: .....

Name of person who made request:.....

Data request received: .....Date acknowledgement sent:.....

Name of person dealing with the request:.....

Check	**Notes**
Is the person requesting information entitled to the data?	
Do you understand what data they are asking for?	
Identify the data	
Collect the required data	
Do you need to exempt/redact data?	
Is the data going to be ready in time?	
Create pack	
Inform requestor you have the data	
Deliver data	

At all stages, your DC or DPL will be able to provide you with advice.

Date request completed:..... Signed off by: .....

Appendix H – *Process for dealing with Freedom of Information (FoI) Requests*

On receiving a Freedom of Information request which must be received in writing the DPO will:

- Inform the DPL and the Head teacher if necessary
- Record the details of the request, updating this record where necessary (see next page).
- Reply to the requestor confirming receipt of the request asking for clarity if there is confusion about which data is required.
- Decide that if the material is already published or falls within an exemption.
- Contact the DPO if clarity on the request is needed or procedure is needed.
- If data is not going to be published inform the requestor why this is not being released.
- Identify the people responsible for gathering the necessary data.
- Gather the data indicating a deadline.
- Examine the data for redactions making sure there is no 'bleeding' of data.
- Ask the requestor for an address and time for delivery.

The whole process should not take any longer than 20 working days.

The Freedom of Information requests are held here: Data Security Folder, in the Office.

Appendix H – *Freedom of information request record*

Name of person who made request:.....

Data request received: ..... Date acknowledgement sent:.....

Name of person dealing with the request:.....

Check	**Comments**
Is the person requesting information entitled to the data?	
Do you understand what data they are asking for?	
Identify the data	
Collect the required data	
Do you own all the data?	
Do you need to exempt/redact data?	
Create pack	
Inform requestor you have the data	
Deliver data	

At all stages, your DC or DPL will be able to provide you with advice.

Date request completed:..... Signed off by: .....

Appendix I – *Data Breach*

Every data protection breach should be recorded. The process that should be followed is listed below:

- Inform the DPL and the Head Teacher immediately.
- Record the details of the breach, updating this record where necessary. The details will need to be shared with Potens' central records of potential and actual breaches.
- DPL to contact and liaise with the DC if clarity on reporting the breach is needed and where necessary, report the breach to the ICO.
- Identify the people whose data has been accidentally released, inform them of the breach and the steps taken to rectify the situation.
- Undertake a full review to identify why the breach took place and establish how future similar events can be avoided.

All Data protection breach records requests are held in the Data Security Folder.
For advice and guidance or raising concerns contact the Information Commissioners Office (ICO)

a. Telephone: 0303 123 1113 or
b. Website: https://ico.org.uk/concerns

Appendix I – Data Breach Record and Log

Date reported	Reported by (Name, Job Title, Service)	Details of Personal Data compromised	Details of how breach occurred/ date of breach	Potential risks identified as result of breach & Risk Mitigation - actions taken	Reported to person(s) affected - include rationale why/ why not	Reported to ICO - include rationale why/ why not	Internal Data Controller informed/ date

POLICY REVIEW RECORD

POLICY NAME	**Information & Data Protection Policy**	
COMPILED BY	Bettina Jeppesen	
DATE	May 2018	
REVIEW DUE DATE	**REVIEWED**	
	DATE	**BY (NAME)** **Items updated**
*Note: Policy review page commenced Feb 2023 only		
	Feb 2023	B Jeppesen Updated Annex D – Privacy Notice for staff, • Added Volunteers • Added reference to SelectHR