Individual Rights

Policy & Procedures

Last Review Date: January 2023

Next Review Date: January 2025

Contents

Policy Statement

The United Kingdom's data protection legislation provides all individuals (data subjects) with certain rights over their personal data. Not all rights are absolute; some may be subject to exemptions.

This document provides staff with information regarding how the Coit & Ecclesfield Primary Federation will fulfil our obligation to facilitate the exercise of data subject rights under the data protection legislation.

This document will direct staff to additional information which may be of assistance where appropriate and provides the contact details for the Schools' Data Protection Leads (DPLs) and the Data Protection Officer (DPO) for additional support. (see Contacts, below)

This policy and procedure should be read in conjunction with the Data Protection Policy.

1. Purpose

The purpose of this procedure is to explain how a data subject can make a ***rights request*** relating to their personal data, as defined in Articles 15 to 21 of the UK GDPR, and how the School will handle ***rights requests*** to ensure compliance with the UK GDPR and any other relevant legislation.

Under this policy and procedure the School:

- knows how to recognise a rights request and we understand when the right applies.
- has a policy for how to record requests we receive verbally.
- understands what steps we need to take to verify the identity of the requester, if necessary.
- understands when we can pause the time limit for responding if we need to ask for clarification.
- understands when we can refuse a request and are aware of the information we need to provide to individuals when we do so.
- understands the nature of the supplementary information we need to provide in response to a subject access request.
- has suitable information management systems in place to allow us to locate, retrieve, rectify, erase, suppress or otherwise cease processing personal data.
- has processes in place to ensure that we respond to rights requests without undue delay and within one month of receipt.

- understands what we need to consider if a third party requests personal data on behalf of another individual.
- is aware of the circumstances in which we can extend the time limit to respond to a request.
- understands how to assess whether a child is mature enough to understand their rights.
- understands what we need to consider if a request includes information about others.
- can transmit personal data in structured, commonly used and machine-readable formats.
- use secure methods to transmit personal data.

2. Scope

This document applies to staff, including temporary staff, agency workers, contractors and others who work for or on behalf of the School. The following rights involving individual rights are covered:

- Article 15: Right of Access (Subject Access Request)
- Article 16: Right of Rectification (Article 16)
- Article 17: Right of Erasure (Right to be forgotten)
- Article 18: Right to Restrict Processing
- Article 20: Right of Data Transfer (Data Portability)
- Article 21: Right to object to processing

3. Responsibilities

All staff, are responsible for adhering to this procedure.

The internal data protection leads are responsible for maintaining a register of all ***rights requests*** and assisting the Data Protection Officer in coordinating the retrieval of information and responses required.

The executive Headteacher together with the Data Protection Officer (DPO) has direct responsibility for maintaining this procedure and providing advice on implementation with the assistance of the relevant staff members as required.

Anyone who is unsure whether they have received a ***rights request*** should contact the DPO as soon as possible. As a general rule, **all requests** related to personal data should be treated as a ***rights request*** until proven otherwise.

4. Definition of Personal Data

Personal data is defined as, ***any information*** relating to an identified or identifiable living individual who can be identified, directly or indirectly from that data.

Personal data includes facts, opinions – whether true or not, or intentions relating to the data subject.

The data protection legislation applies to personal data which;

- is processed wholly or partly by automated means e.g. IT systems, CCTV, voicemail, etc.
- forms or intended to form part of a filing system, e.g., a categorised file that enables personal data to be readily accessible.

For further details on what constitutes personal data please see here

A visual aid may be found in Appendix 2

5. Receiving a Valid Request

A data subject (an individual whose information is processed by the Schools), may make a ***rights request*** via any communications medium used by the Schools.

Staff should be able to identify a potential ***rights request*** regardless of the method of communication. As a general rule staff should treat ***any*** request relating to personal data as a ***rights request*** until proven otherwise. Requests may be received by:

- Phone or face-to-face (verbal)
- Email
- Written (letter)
- Website contact forms
- Schools communications apps
- Social media channels

An **Individual *Rights Request Form*** is available on request from the office by contacting enquiries@ecclesfield-pri.sheffield.sch.uk

Use of the ***rights request*** form ***is not compulsory*** for the data subject.

To ensure consistency in the recording and process management of ***rights requests*** staff should use the form to record any ***rights request*** received verbally or by other means. The original written request (email, letter, etc.) should be attached to the form for reference.

6. Verifying the Identity of the Data Subject

Data Protection legislation requires the School to take 'reasonable measures' to verify the

identity of a data subject. Often verification of identity can be determined by comparing personal information in the ***rights request*** with data held by the School. For example, is the name and signature or address on the request the same as that held on internal records?

If the School cannot reliably verify the data subject's identity from the information provided, further steps are required:

Verifying identity by phone

Telephone the data subject to confirm they have made the ***rights request*** and ask them several questions based on the information held by the School to confirm their identity.

Verifying identity by letter

If verification of identity by phone has failed, or if the School is not satisfied that the identity of the data subject has been confirmed, the School may ask the individual to verify their identity and address by providing one document from ***each*** category:

(a) Photographic confirmation:

- full driving licence, passport, another official photographic id

(b) Confirmation of name and address:

-utility bill, bank or credit card statement, or an equivalent/similar official document – the document **MUST** show the data subject's name and address.

Once the School is satisfied a note will be made that this requirement has been met and any copies of identification documents will be shredded (there is no requirement to retain copies of any ID verification). If original documents have been provided these must be returned in person or posted back via recorded delivery.

If the School does not receive verification of identity, or it is still not satisfied as to the identity of the Requestor then the **rights request** should not be complied with and a refusal notice should be issued.

7. Requests from parties other than the data subject

There are occasions where a data subject may agree to a third party, such as a family member or a solicitor, making a ***rights request*** on their behalf.

To protect a data subject's personal data, the School will make all reasonable checks to be satisfied that the individual making the request on behalf of the data subject is entitled to do so. This may include requesting a written authority (e.g. evidence of consent from the individual), or a more general power of attorney.

It is the third party's responsibility to provide evidence of their authority. The authorisation request should therefore be made directly to the third party, not to the data subject.

No information should be released until the School is satisfied that the third party is acting with the authority of the data subject.

8. Requests on behalf of a child

Personal data belongs to the data subject, and in the case of the personal data of a child regardless of their age the rights concerning that personal data are theirs and not those of their parents. Parents, in most cases, do not have automatic rights to the personal data of their children.

However, there are circumstances where a parent may exercise data subject rights on behalf of the child without requiring the consent of the child. Generally, when a child is under 12 years of age, they are deemed not mature enough to understand their data subject rights and a parent/carer may exercise those rights on their behalf.

If a child is 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child cannot make an access request on their own behalf, the School will require the written authorisation of the child before permitting the parent/carer to act on the child's behalf.

In all cases the School will consider the particular circumstances of the case and act accordingly; the above are guidelines only.

9. Charges

In most cases, there will be **no fee** charged for responding to a rights request. However, where the School can demonstrate that the request is manifestly unfounded or excessive it can either;

- charged a reasonable fee, reflective of the administrative costs of dealing with the request; or
- refuse to act on the request.

The data subject or their authorised representative will be informed of such a decision, the reason why, and how a complaint may be raised with the Information Commissioner's Office (ICO) if the data subject wishes to appeal the decision.

If the request relates to access to personal data, where the School has provided one copy of the personal data free of charge, a reasonable fee may be charged for additional copies based on administrative costs.

10. Timescales

The School shall provide a response to the data subject or their representative without undue delay and in any event within ***one calendar month*** of receipt of a valid ***rights request***.

This period may be extended by two further months where necessary, considering the complexity and number of requests.

The Data Protection Officer shall inform the data subject of any extension within one calendar month of receipt of the request, together with the reasons for the delay.

A calendar month is defined as the equivalent date in the subsequent month. For example, if a

request is received on the 5th of February, it must be fulfilled by the 5th of March.

If it is not possible to comply with the request; for example the information requested does not fall within the scope of a rights request, or the information is not held by the School, or the information is subject to an exemption (see below), the Data Protection Officer shall inform the data subject without undue delay and at the latest within one calendar month of receipt of the request of the reason/s for not progressing the rights request and the right to complain to the ICO.

11. Responding to Requests

The data provided in any response shall be presented in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Where an email or online request for copy data is received, the data shall be provided by email, unless the data subject has specifically requested that it be provided in another form.

The transfer of personal data from the School to the data subject or their authorised representative shall be subject to appropriate security measures in transit.

12. Access Requests (Subject Access Requests)

This right enables a data subject to verify that School s lawfully processing their personal data and to check its accuracy.

Where data is being processed by the School and the data subject requests access to their own personal data, the School shall provide the access together with supplementary data including:

- the purpose of the processing
- the categories of personal data being processed
- the recipients or categories of recipients to whom we have disclosed or will disclose personal data;
- the retention period for the data (or how we determine that);
- the existence of the right to rectification, erasure or restriction of processing of that data;
- the source of the information if it was not collected directly from the data subject; and
- the existence of any automated decision-making or processing, if relevant.
- the right to lodge a complaint with the ICO
- where personal data are transferred to a third country or international organisation, the appropriate safeguards relating to the transfer, if relevant.

The School must ensure other individuals' personal data is treated fairly and protected

accordingly. Therefore, before the School releases anything to the data subject or representative it has to ensure that it's not inappropriately releasing information about other individuals who can be identified from that information.

On occasions where somebody else can be identified from that information, the School will take one or more of the appropriate approaches below to protect the personal data of third parties:

- Seek documented consent from the other individuals concerned
- Where appropriate redact information so other individuals cannot be identified
- Where appropriate provide a summary of the personal data
- Review whether it would be reasonable to release the information without consent. Considering; is the information already known by the data subject? Is the individual acting in their professional capacity and having dealings with the data subject? Is there a duty of confidentiality owed to the other individual?

The data subject's interests and those of the other individuals will be reviewed and considered on a case-by-case basis.

The Data Protection Act 2018 makes it an offence to intentionally alter, deface, block, erase, destroy or conceal information to prevent disclosure of all or part of the information that the person making the request would have been entitled to receive.

For further information and guidance please see here

13. Rectification Requests

Under Article 16 of the UK GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed.

The UK GDPR does define the term 'accuracy'. However, the Data Protection Act 2018 states that personal data is inaccurate if it is "*incorrect or misleading as to any matter of fact*".

Where the request is for the rectification of inaccurate personal data, the School will restrict (stop) further processing of the contested personal data while its accuracy is verified.

Where the rectification request is upheld, and if the data has previously been shared with any third parties, those third parties will be instructed as to the necessary rectifications. An exception to notifying third parties exists where notification proves impossible or involves disproportionate effort.

If the School is satisfied that the personal data is accurate, the data subject should be informed that the data will not be amended. The School should explain its decision, and inform the data subject of their right to make a complaint to the ICO; and their ability to seek to enforce their rights through a judicial remedy.

It is also good practice to place a note on your system indicating that the data subject challenges the accuracy of the data and their reasons for doing so.

For further information and guidance please see here

14. Erasure Requests

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

This right can only be exercised by data subjects where the School:

- no longer requires the data for the purpose for which it was originally collected
- relies on consent as the lawful basis for holding the data, and the individual withdraws their consent
- relies on legitimate interests as the lawful basis for processing and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing
- are processing the personal data for direct marketing purposes and the individual objects to that processing
- has processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle)
- has to comply with a legal obligation; or
- has processed the personal data to offer information society services to a child.

Where personal data is to be deleted, data held in different locations and formats must be reviewed to ensure that all relevant personal data is erased.

Where the School have made personal data public, it shall take reasonable steps (taking to account technology and cost), to notify other controllers processing the data of the data subject's request for erasure.

Erasure of Children's data

The School acknowledges the enhanced protection of children's information, especially in online environments and will give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet (social media channels, websites, etc.)

For specific information and guidance about the right to erasure and children's personal data please see here

The School is not required to and will not delete personal data where the processing carried out is necessary for:

- exercising the right of freedom of expression
- complying with a legal obligation in the public interest or the exercise of an official authority

- for public health reasons
- for archiving purposes; or
- for the establishment, exercise or defence of legal claims.
- The UK GDPR also specifies two circumstances where the right to erasure ***will not apply*** to special category data:
- if the processing is necessary for public health purposes in the public interest; or
- if the processing is necessary for preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

Where the erasure request ***is upheld***, the School shall inform any third parties with whom the personal data has been shared, unless this proves impossible or involves disproportionate effort. If asked to do so, the School must also inform the data subjects about these recipients.

Once the relevant personal data have been deleted the data subject shall be advised that the data has been erased unless doing so is impossible or involves disproportionate effort.

Where the erasure request ***is not upheld*** the data subject should be informed that the data will not be erased. The School should explain its decision, and inform the data subject of their right to make a complaint to the ICO; and their ability to seek to enforce their rights through a judicial remedy.

For further information and guidance please see here

15. Restriction Requests

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that the School uses their data. This is an alternative to requesting the erasure of their data.

The right to restriction is not an absolute right and the data subject will only be entitled to restriction where:

- the accuracy of personal data is contested by the data subject for a period to enable the School to verify the accuracy of the data
- the processing is unlawful, and the data subject does not want it to be erased but requests restriction instead
- the School no longer need the data, but the data is required by the data subject for the

establishment, exercise or defence of legal claims; or

- the processing has been objected to and verification of that objection is pending.

Where the data subject exercises their right to restriction, that personal data can only be processed with their consent, or for the establishment, exercise or defence of legal claims, or for the protection of rights in the public interest, or for the protection of the rights of another data subject or legal entity.

Where the School have restricted any form of processing and that restriction is subsequently to be lifted, the data subject should be advised accordingly unless doing so is impossible or involves disproportionate effort.

16. Data Portability (Transfer Requests)

This right allows a data subject to obtain and reuse personal data for their own purposes across different services.

The data subject may request a copy of their personal data to transfer it from the School to another data controller where:

- the lawful basis for processing is consent or a contract with the data subject; and,
- the processing is carried out by automated means (electronically, this right does not apply to paper records).

The data subject shall only be provided with the personal data they have provided to the School including personal data gathered in the course of the relationship with the data subject, or which has been generated from monitoring of the data subject's activity.

The data subject is entitled to be provided with their personal data in a structured, commonly used and machine-readable format for transfer to another controller; or where possible to have the School transfer the data directly to another controller.

For more information and guidance please see here

17. Objection Requests

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Whether the right applies depends on the School's purposes and the lawful basis for processing.

Individuals have the ***absolute right*** to object to the processing of their personal data if it is for direct marketing purposes. Where such a request is received, the School must comply with the request immediately.

Individuals may also object if the processing is for:

- a task carried out in the public interest;

- the exercise of official authority vested in you; or
- legitimate interests (or those of a third party). The School ***may not*** use 'legitimate interest' as a lawful basis for processing where it is acting in its official capacity.

If the School can demonstrate it has legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or the processing is necessary for the establishment, exercise or defence of legal claims, it is not necessary to cease processing.

For further information and guidance please see here

18. Exemptions

The Data Protection Act 2018 provides exemptions from the obligation to w respond to data subject rights in certain circumstances.

Careful consideration should be given to these exemptions and whether they apply, before responding to any rights request.

The exemptions from compliance with rights requests are set out in Schedules 2, 3 and 4 of the Data Protection Act (2018).

In summary, these are:

Crime and taxation – for the prevention or detection of crime; the apprehension or prosecution of offenders or the assessment or collection of tax or duty or imposition of a similar nature to the extent that those provisions would prejudice the activity.

Immigration – for the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control.

Information required to be disclosed by law etc. or in connection with legal proceedings – to the extent that the application of the provisions would prevent same including disclosure which is necessary for or in connection with legal proceedings (including prospective legal proceedings), or for obtaining legal advice or otherwise establishing, exercising or defending legal rights.

Functions designed to protect the public – certain functions carried out to protect the public from financial loss through fraud etc.; to protect charities; for health and safety reasons; to prevent malpractice in a public office; or to protect business interests.

Regulatory activity – relating to certain bodies where the application of the provisions would prejudice the discharge of their function.

Legal professional privilege/confidentiality of communications – some solicitor/client communications or information prepared for litigation

Self-incrimination – to the extent that complying would reveal evidence of an offence

Corporate finance – in certain circumstances

Management forecasts - to the extent that the application of the provisions would prejudice the conduct of the business or activity concerned

Negotiations - with the data subject to the extent that the application of the provisions would prejudice those negotiations

Confidential references - given to or provided by the School

Health, social work, education and child abuse data to the extent that the application of the provisions would cause prejudice.

19. Register of Requests

The internal Data Protection Lead (DPL) is responsible for maintaining a register of requests and relevant records to permit monitoring of the progress of requests, the volume of requests received, and compliance with the UK GDPR.

20. Records Retention

A copy of all the data retrieved must be taken for reference should the data be challenged by the data subject. These will be maintained in line with the records retention schedule and retained for 1 year.

21. Complaints / Right of Appeal

If the data subject or their representative is not satisfied with the outcome of their rights request, in the first instance, the individual will be encouraged to contact the Data Protection Officer.

If they are still not satisfied they can contact the Information Commissioner's Office directly at Information Commissioner's Office, Wycliffe House Water Lane Wilmslow Cheshire. SK9 5AF. Tel: 0303 123 0003

E-mail: casework@ico.org.uk Website: www.ico.org.uk

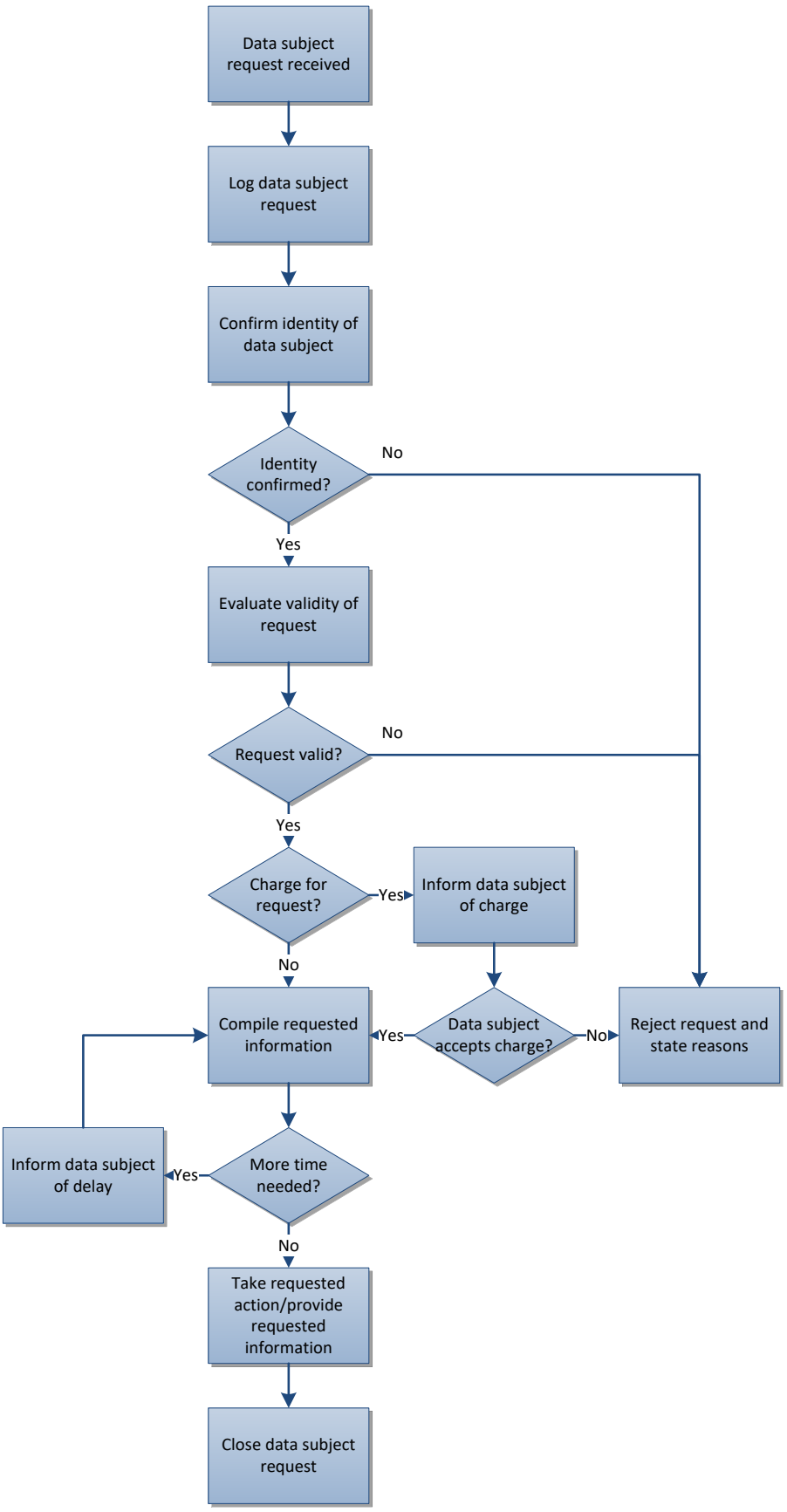
22. Contacts

Headteacher:	**J.Eagleton**
Email:	**enquiries@ecclesfield.sheffield.sch.uk**
Phone:	**01142468710**

Data Protection Lead:	**Hannah Travers**
Email:	**enquiries@ecclesfield.sheffield.sch.uk**
Phone:	**01142468710**

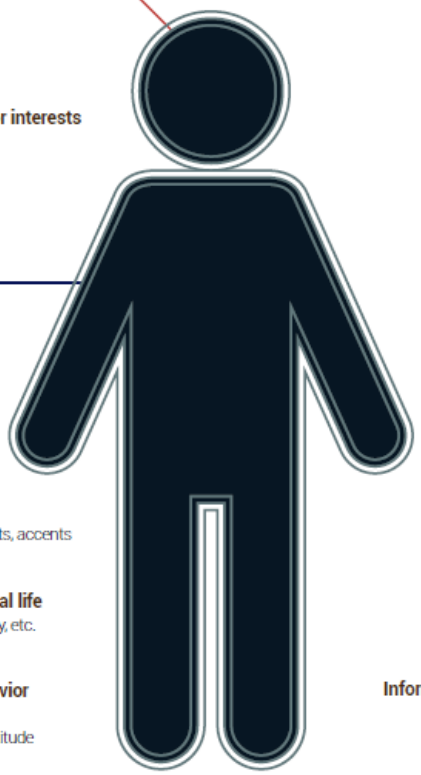
Data Protection Officer:	**Dee Whitmore**
Email:	**dposervice@schoolspeople.co.uk**
Phone:	**01142467396**

Appendix 1: Rights Request: Procedure Flowchart



Appendix 2: Categories of Personal Data

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.



INTERNAL

Knowledge and Belief
Information about what a person knows or believes
religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks

Authenticating
Information used to authenticate an individual with something they know
passwords, PIN, mother's maiden name

Preference
Information about an individual's preferences or interests
opinions, intentions, interests, favorite foods, colors, likes, dislikes, music

EXTERNAL

Identifying
Information that uniquely or semi-uniquely identifies a specific individual
name, user-name, unique identifier, government issued identification, picture, biometric data

Ethnicity
Information that describes an individual's origins and lineage
race, national or ethnic origin, languages spoken, dialects, accents

Sexual
Information that describes an individual's sexual life
gender identity, preferences, proclivities, fetishes, history, etc.

Behavioral
Information that describes an individual's behavior or activity, on-line or off
browsing behavior, call logs, links clicked, demeanor, attitude

Demographic
Information that describes an individual's characteristics shared with others
age ranges, physical traits, income brackets, geographic

Medical and Health
Information that describes an individual's health, medical conditions or health care
physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions

Physical Characteristic
Information that describes an individual's physical characteristics
height, weight, age, hair color, skin tone, tattoos, gender, piercings

HISTORICAL

Life History
Information about an individual's personal history
events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)

FINANCIAL

Account
Information that identifies an individual's financial account
credit card number, bank account

Ownership
Information about things an individual has owned, rented, borrowed, possessed
cars, houses, apartments, personal possessions

Transactional
Information about an individual's purchasing, spending or income
purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits

Credit
Information about an individual's reputation with regards to money
credit records, credit worthiness, credit standing, credit capacity

SOCIAL

Professional
Information about an individual's educational or professional career
job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions

Criminal
Information about an individual's criminal activity
convictions, charges, pardons

Public Life
Information about an individual's public life
character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data

Family
Information about an individual's family and relationships
family structure, siblings, offspring, marriages, divorces, relationships

Social Network
Information about an individual's friends or social connections
friends, connections, acquaintances, associations, group membership

Communication
Information communicated from or to an individual
telephone recordings, voice mail, email

TRACKING

Computer Device
Information about a device that an individual uses for personal use (even part-time or with others)
IP address, Mac address, browser fingerprint

Contact
Information that provides a mechanism for contacting an individual
email address, physical address, telephone number

Location
Information about an individual's location
country, GPS coordinates, room number