LANCASTER
STEINER SCHOOL

Data Protection Policy

Version date: June 2022

Document review period: March – May 2024

CONTENTS

Contents

1. AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill .

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and of the Data Protection Act 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR .

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ● Name (including initials) ● Address Identification number ● Location data ● Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ● Racial or ethnic origin ● Political opinions ● Religious or philosophical beliefs ● Trade union membership ● Genetics ● Biometrics (such as fingerprints, retina

	and iris patterns), where used for identification purposes ● Health – physical or mental ● Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Data protection officer (DPO)	A DPOs assists with monitoring internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, trustees, visitors and others, and therefore is a data controller. We do not require a DPO as our organisation is not using data in a scale large enough to meet the criteria to need one. The school is registered with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 BOARD OF TRUSTEES

The Board of Trustees has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 SCHOOL MANAGEMENT TEAM

The School Management Team acts as the representative of the data controller on a day-to-day basis.

5.3 ALL STAFF

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the school office in the following circumstances:
    - o With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - o If they have any concerns that this policy is not being followed
    - o If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - o If they need to rely on or capture consent, draft a privacy notice , deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - o If there has been a data breach
    - o Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - o If they need help with any contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school must comply with. The principles say that personal data must be:

● Processed lawfully, fairly and in a transparent manner

● Collected for specified, explicit and legitimate purposes

● Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed

● Accurate and, where necessary, kept up to date

● Kept for no longer than is necessary for the purposes for which it is processed

● Processed in a way that ensures it is appropriately secure

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSONAL DATA

7.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**

- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the **public interest**.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.2 LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

When staff no longer needs the personal data they hold, they must ensure it is deleted or anonymised.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

● There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

● We need to liaise with other agencies – we will seek consent as necessary before doing this

● Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law

o Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

o Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

● The prevention or detection of crime and/or fraud

● The apprehension or prosecution of offenders

● The assessment or collection of tax owed to HMRC

● In connection with legal proceedings

● Where the disclosure is required to satisfy our safeguarding obligations

● Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email the School Manager They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to School Manager

9.2 CHILDREN AND SUBJECT ACCESS REQUESTS

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions

taken with no human involvement, that might negatively affect them)

- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the School Manager. If staff receive such a request, they must immediately forward it to the School Manager.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents/carers do not have an automatic legal right to access to their child's educational record. If a parent would like to request access, by writing to the School Manager. A charge may apply.

11. BIOMETRIC RECOGNITION SYSTEMS

Lancaster Steiner School does not use any form of biometric system.

12. CCTV

Lancaster Steiner School do not currently use CCTV. However if they are installed in the future, we may use CCTV in various locations around the school site to ensure it remains safe and would adhere to the ICO's code of practice for the use of CCTV.

13. PHOTOGRAPHS AND VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

For children under 12, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers,

campaigns

● Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified .

14. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

● Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

● Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies

● Integrating data protection into internal documents including this policy, any related policies and privacy notices

● Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance

● Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

● Maintaining records of our processing activities, including:

o For the benefit of data subjects, making available all information we are required to share about how we use and process their personal data (via our **privacy notice)**

o For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

● Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

● Papers containing confidential personal data must not be left on office and classroom desks, on

staff room tables, pinned to notice/display boards, or left anywhere else where there is general access

● Where personal information needs to be taken off site, staff must sign it in and out from the school office

● Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

● Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.

● Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

● Safeguarding information being made available to an unauthorised person

● The theft of a school laptop containing non-encrypted personal data about pupils

18. TRAINING

All staff and trustees are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. MONITORING ARRANGEMENTS

The School Manager is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every 2 years.

20. LINKS WITH OTHER POLICIES/DOCUMENTS

This data protection policy is linked to our:

- Acceptable Use (ICT) Policy
- Code of Conduct for All Adults in School
- Use of Image Policy
- Online Safety Policy

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

● On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the school office

● The office staff will investigate the report, and determine whether a breach has occurred. To decide, the office staff will consider whether personal data has been accidentally or unlawfully:

- o Lost
- o Stolen
- o Destroyed
- o Altered
- o Disclosed or made available where it should not have been
- o Made available to unauthorised people

● The office staff will alert the Senior Management Team and the chair of trustees

● The Management Team and Trustees will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

● The Management Team and Trustees will assess the potential consequences, based on how serious they are, and how likely they are to happen

● The Management Team and Trustees will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Management Team and Trustees will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- o Loss of control over their data
- o Discrimination
- o Identify theft or fraud
- o Financial loss
- o Unauthorised reversal of pseudonymisation (for example, key-coding)
- o Damage to reputation
- o Loss of confidentiality

o Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the Management Team and/or Trustees must notify the ICO.

● The Management Team and/or Trustees will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored under 'GDPR' in the Clerical shared drive.

● Where the ICO must be notified, the Management Team and/or Trustees will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

o A description of the nature of the personal data breach including, where possible:

▪ The categories and approximate number of individuals concerned

▪ The categories and approximate number of personal data records concerned

o The name and contact details of the Management Team and/or Trustees dealing with the breach

o A description of the likely consequences of the personal data breach

o A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

● If all the above details are not yet known, the Management Team and/or Trustees will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when they expect to have further information, submitting the remaining information as soon as possible

● Management Team and/or Trustees will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, they will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

o The name and contact details of Management Team and/or Trustees dealing with the breach

o A description of the likely consequences of the personal data breach

o A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

● Management Team and/or Trustees will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

● Management Team and/or Trustees will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

o Facts and cause

o Effects

o Action taken to contain it and ensure it does not happen again (such as establishing

more robust processes or providing further training for individuals)

● Records of all breaches will be stored under 'Data Protection' in the Admin Store.

● The Management Team and/or Trustees will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

● If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

● Members of staff who receive personal data sent in error must alert the sender and the School Office as soon as they become aware of the error

● If the sender is unavailable or cannot recall the email for any reason, the office staff or management team will ask the IT committee to recall it

● In any cases where the recall is unsuccessful, the office staff or management team will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

● The Management Team and/or Trustees will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request

● The Management Team and/or Trustees will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted. For example:

● Non-anonymised staff pay information

● A school laptop containing non-encrypted sensitive personal data being stolen or hacked

APPENDIX 2: PRIVACY NOTICE

Our contact details

Name: The School Office

Address: Lune Road, Lancaster LA15QU

Website: lancastersteinerschool.org

Phone Number: 01524 381876

Date: 15/06/2022

E-mail: enquiries@lancastersteinerschool.org

The type of personal information we collect

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name, contact details for parents, children, emergency contacts, customers and suppiers)
  - Names and contact details
  - ID in the form of passports, certificates or financial documents
  - Medical, educational, health and safety and dietary information (including attendance)
  - Photographic and video imagery

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- To administer children to and from our school and comply with our obligations to Lancaster County Council
- To create financial agreements for school fees
- To conduct recruitment related processes
- To enable us to administer our website and perform marketing functions

We also receive personal information indirectly, from the following sources in the following scenarios:

- Schools previously attended by pupils to provide continuity of care for children joining our school from another setting.
- Previous employers, disclosure and barring service or referees when employing new staff or vetting volunteers
- Other professional organisations for example Social Services, NHS or the Police may share relevant information with us so that we can support your child and/or families needs.

We use the information that you have given us in order to:

- Understand your childs and/or families medical, educational or safeguarding needs.
- Complete our employment and vetting processes
- Enable us to meet out health and safety requirements

We may share this information with:

- Other schools as part of your child transfer to another school
- Other professional organisations, for example Social Services, Police, NHS, Lancashire County Council or a Safeguarding representative (for example, LADO).

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:

(a) Your consent. You are able to remove your consent at any time. You can do this by contacting: enquiries@lancastersteinerschool.org

(b) We have a contractual obligation to process this information.

(c) We have a legitimate interest to process this information.

How we store your personal information

Your information is securely stored.

We keep all personal information collected either in a locked filing cabinet or electronically and protected by passwords. All personal information is only kept for as long as necessary. At which time we will then dispose of your information by shredding paper copies and erasing data stored electronically.

Any data on devices which are being disposed of will have their data erased using a data disposal and shredding company/device to ensure all personal data is non-recoverable.

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at either enquiries@lancastersteinerschool.org, 01524381876 or Lancaster Steiner School, Lune Road, Lancaster, LA1 5QU if you wish to make a request.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at Lancaster Steiner School, Lune Road, Lancaster, LA1 5QU or email enquires@lancastersteinerschool.org for data protection queries.

You can also complain to the Information Commissioner's Office (ICO) if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

APPENDIX 3: USEFUL LINKS

USEFUL LINKS:

General Data Protection Regulation (GDPR)

The Data Protection Bill

Guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests .

APPENDIX 4: DATA PROTECTION DECLARATION

I_____(full name) confirm I have read and

understand the Lancaster Steiner School Data Protection Policy. If I have any

questions I should speak to the School Manager or consult

the policy in the office binder where further information is held.

Signed:

Date: