URSULINE HIGH SCHOOL
Wimbledon

Data Protection Policy

January 2024

HEADTEACHER MR EOIN KELLY BA Hons, MSC, PGCE

URSULINE HIGH SCHOOL CRESCENT ROAD WIMBLEDON LONDON SW20 8HA

TEL: 020 8255 2688 FAX: 020 8255 2687
E-MAIL: enquiries@ursulinehigh.merton.sch.uk
WEBSITE: www.ursulinehigh.merton.sch.uk

Data Protection Policy

Contents

1. Introduction

1.1 The Data Protection Act (DPA) 2018 and the General Data Protection Regulations (GDPR) provide the law which safeguards personal privacy, giving protection for individuals as to how their personal information is used. It applies to anyone who handles or has access to people's personal data.

1.2 Schools are required to have a data protection policy which must comply with the GDPR. This is because every school is classed as a Data Controller under the data protection legislation because they decide how personal data for which they are responsible is processed. Each school and every employee has a legal duty to protect the privacy of information relating to individuals that it processes.

1.3 This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR) 2018
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Data Protection Bill 2017-19 which will adopt the GDPR, DPLED and The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data into UK law in the wake of the UK's exit from the European Union.

This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner' Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- Department For Education (2018) 'Data Protection: A toolkit for schools'

2. Policy objectives

2.1 This policy is intended to ensure that Ursuline High School's personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

2.2 The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

2.3 All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All members of staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities.

3. Information Covered

3.1 Personal data is defined under the GDPR as "any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier held by the school."

3.2 The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

3.3 Ursuline High School collects and uses a large amount of personal information every year about staff, students, parents and other individuals who come into contact with the school. By way of example, this includes student records, staff records, names and addresses of those requesting prospectuses, test marks, references and fee collection. of Local Authorities (LAs), government agencies and other bodies. In addition, there may be a legal requirement for the School to process personal information to ensure that it complies with statutory obligations.

3.4 The information collected is processed in order to enable the school to provide education and other associated functions.

4. Key Principles

4.1 Data Protection Principles – there are six enforceable principles contained in Article 5 of the General Data Protection Regulations, which the School must adhere to when processing personal data.

- Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency)
- Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
- Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (data minimisation)
- Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay. (accuracy)
- Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. (storage limitation)
- Principle 6 (the Security Principle) - Personal data shall be processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data, using appropriate technical or organisational measures.(integrity and confidentiality)

4.2 There is a 7th Principle - the Accountability Principle which requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. At the school, the responsibility for adherence to the principles lies with all school staff.

4.3 The organisation must have appropriate measures and records in place to be able to demonstrate their compliance.

4.4 In addition to adherence to the principles, there are transfer limitations relating to the transfer of personal data to a country outside the EEA. Should an occasion arise

requiring such a transfer, members of staff should contact the Data Protection Officer for assistance.

4.5 Overall commitment to compliance with the above principles.

4.6 Alongside actions relating to specific obligations with which the legislation obliges the school to comply, and which are included below in relevant sections of this Policy, the school will:

(a) Produce an information asset register that contains details of the records it holds.

(b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.

(c) Inform individuals when their information is shared, and why and with whom it will be shared.

(d) Check the quality and the accuracy of the information it holds.

(e) Ensure that information is not retained for longer than is necessary.

(f) Ensure that when obsolete, information is destroyed and it is done so appropriately and securely.

(g) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.

(h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

(i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information.

(j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings,

provided that the disclosure falls within an exemption to the non-disclosure provisions contained within the Data Protection Act 1998 or any subsequent legislation.

(k) Disclose personal data where required to do so by law for example, following receipt of a court order.

(l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:

- request access to personal information, known as Subject Access Requests.
- be informed about the way their data is used;
- have inaccurate personal data rectified;
- have their personal data erased;
- restrict the processing of their personal data; and
- object to the processing of their personal data.

(m) Ensure the school's staff are appropriately and regularly trained and aware of and understand the school's policies and procedures.

(n) Create and maintain a data breach notification spreadsheet to record data breaches and also circumstances where a breach was narrowly avoided

.

5. Lawful Basis for processing personal information (Article 6 GDPR)

5.1 Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing, must be selected by the school.

5.2 The lawful basis for processing which has been selected must be recorded, to demonstrate compliance with the data protection principles, and include information about the purpose of the processing and the justification for why you believe this basis applies.

5.3 The lawful bases

(a) The data subject has given consent to the processing of his or her data for one or more specific purposes. (Consent)

(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (Contract)

(c) Processing is necessary for compliance with a legal obligation to which the data controller is subject. (Legal Obligation)

(d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person. (Vital interests)

(e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school (Public Task)

(f) Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. (Legitimate Interests) N.B. This basis does not apply to processing carried out by public authorities in the performance of their tasks. However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate.

5.4 Where the lawful basis for processing is consent this must be clearly evidenced by a very clear and specific statement. Such consent requires a positive opt-in and so pre-ticked boxes or any other method of default consent will not be sufficient. If consent is given in a document which deals with other matters, the consent must be kept separate from those other matters. The data subject shall have the right to withdraw his or her consent at any time and withdrawal must be promptly honoured. Prior to giving consent, the data subject shall be notified of the right of withdrawal.

5.5 Processing of special categories of personal data – Article 9

5.5.1 Processing of sensitive personal information is prohibited unless a lawful special condition for processing is identified. It comprises data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or which concerns health or is genetic or biometric data which uniquely identifies a natural person.

5.5.2 Such personal data will only be processed by the school if:

(a) There is a lawful basis for doing so as identified in Article 6.

(b) One of the special conditions for processing sensitive personal information applies:

(i) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
(ii) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
(iii) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
(iv) the processing is carried out during its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
(v) the processing relates to personal data which are manifestly made public by the data subject
(vi) the processing is necessary for the establishment, exercise or defence of legal claims
(vii) the processing is necessary for reasons of substantial public interest
(viii) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
(ix) the processing is necessary for reasons of public interest in the area of public health.

(c) The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

5.6 Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

5.7 Unless the school can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. In such circumstances the school will obtain evidence of and record consent so that it can demonstrate compliance with the GDPR.

6. Data Protection Officer (DPO)

6.1 The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data, for example, the Head Teacher, or Head of Information Technology. For this reason, we have appointed:

Name: Mr Crabtree

Address: London Borough of Merton

Email: schoolsdpo@merton.gov.uk

7. Data Protection Impact Assessments (DPIA)

7.1 The school will carry out a DPIA when processing is likely to result in high risk to the data protection rights and freedoms of individuals.

7.2 The GDPR does not define high risk but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include

7.2.1 the use of new technologies,

7.2.2 processing on a large scale,

7.2.3 systematic monitoring,

7.2.4 processing of special categories of personal data.

7.3 The purpose of the DPIA is to assess:

7.3.1 whether the processing is necessary and proportionate in relation to its purpose

7.3.2 the risks to individuals, including both the likelihood and the severity of any impact on them

7.3.3 what measures can be put in place to address those risks and protect personal information.

7.4 Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template. When carrying out a DPIA they should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

8. Documentation and Records

8.1 The school in accordance with its duty as a Data Controller and Data Processor will keep detailed records of data processing activities and the records shall contain: -

(a) the name and contact details of the school

(b) the name and contact details of the School's Data Protection Officer

(c) the name and details of individuals or roles that carry out the processing

(d) the purposes of the processing

(e) a description of the categories of individuals i.e. the different types of people whose personal data is processed

(f) categories of personal data processed

(g) categories of recipients of personal data

(h) details of any transfers to third countries, including documentation of the transfer mechanism safeguards in place

(i) retention schedules

(j) a description of technical and organisational security measures

8.2 The school will make these records available to the Information Commissioner's Office (ICO) upon request and will, on an annual basis, provide its registrable particulars and pay the data protection fee to the ICO.

8.3 As part of the school's record of processing activities the DPO will document, or link to documentation on:

(a) information required for privacy notices such as:

(b) the lawful basis for the processing

(c) the legitimate interests for the processing

(d) individuals' rights

(e) the source of the personal data

(f) records of consent

(g) controller-processor contracts

(h) the location of personal data

(i) DPIA reports and

(j) records of personal data breaches.

8.4 Records of processing of sensitive information are kept on:

(a) the relevant purposes for which the processing takes place, including why it is necessary for that purpose

(b) the lawful basis for the processing and

(c) whether the personal information is retained or has been erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

8.5 The School will conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

(a) Carrying out information audits to find out what personal information is held

(b) Talking to staff about their processing activities

(c) Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

9. Privacy Notices

9.1 A privacy notice under the GDPR should include:

(a) The school's name and contact details

(b) The contact details of the DPO

(c) The personal data you are collecting & why you are collecting it

(d) Where you get the personal data from & who you are sharing it with

(e) The lawful basis for processing the data

(f) How long the data will be held for

(g) Description of the data subjects' individual rights

(h) The data subjects right to withdraw consent for the processing of their data

(i) How individuals can complain

9.2 The school will publish an overarching privacy notice, which will be posted on its website, which will provide information about how and why the school gathers and uses images and shares personal data.

9.3 In addition to publication of that notice, the school will also issue privacy notices, to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation of why the information is being requested and the purpose for which it will be used.

9.4 The school will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

9.5 The school will issue a minimum of two privacy notices, one for student information, and one for workforce information, and these will be reviewed at regular intervals to ensure they reflect current processing and are in line with any statutory or contractual changes.

9.6 The privacy notices will be amended to reflect any changes to the way the school processes personal data.

9.7 The privacy notice will include details of whether it intends to use biometric data and how consent will be requested to do this and include details of the school's policy regarding photographs and electronic images of pupils.

10. Data Minimisation

10.1. Purpose Limitation

The school will ensure that personal data

(a) is only collected for specified, explicit and legitimate purposes

(b) is not further processed in any manner incompatible with those purposes

(c) is not used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

10.2 Data minimisation

10.2.1. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

10.2.2. Staff may only process data when their role requires it. Staff will not process personal data for any reason unrelated to their role.

10.2.3. The school maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.

10.2.4 Staff will take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

10.2.5. The school will ensure that data subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

11. Individual Rights and Responsibilities

11.1 Individual rights

The school will observe the following rights which staff as well as any other 'data subjects' enjoy in relation to their personal information:

(a) To be informed about how, why and on what basis that information is processed (see the relevant privacy notice)

(b) To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request

(c) To have data corrected if it is inaccurate or incomplete

(d) To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')

(e) To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but the individual(s) concerned does/do not want the data to be erased) or where the school no longer needs the personal information, but the individual(s) require(s) the data to establish, exercise or defend a legal claim

(f) To restrict the processing of personal information temporarily where they do not think it is accurate (and the school is verifying whether it is accurate), or where they have objected to the processing (and the school is considering whether the school's legitimate grounds override the individual's(s') interests)

(g) In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format

(h) To withdraw consent to processing at any time (if applicable)

(i) To request a copy of an agreement under which personal data is transferred outside of the EEA.

(j) To object to decisions based solely on automated processing, including profiling

(k) To be notified of a data breach which is likely to result in high risk to their rights and obligations

(l) To make a complaint to the ICO or a Court.

11.2 Individual Responsibilities

During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If members of staff have access to personal information, they must:

(a) only access the personal information that they have authority to access and only for authorised purposes

(b) only allow other staff to access personal information if they have appropriate authorisation

(c) only allow individuals who are not school staff to access personal information if they have specific authority to do so

(d) keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).

(e) not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device

(f) not store personal information on local drives or on personal devices that are used for work purposes.

12. Photographs and Electronic Images

12.1 CCTV: The school uses CCTV in various locations around the to ensure it remains safe. The school will adhere to the ICO's Code of Practice for the use of CCTV.

There is no requirement to ask individuals' permission to use CCTV. Any enquiries about the CCTV system should be directed to the DPO.

12.2 Photographs and Videos: As part of the school's activities, we or a 3rd party (e.g. school photographers) may want to take photographs and record images of individuals within the school.

The school will obtain consent from parents/carers for photographs and videos to be taken of their daughter/son for communication, marketing and promotional materials.

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.

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

13. Access to Personal Data & Subject Access Requests

13.1 This section sets out the process that will be followed by the school when responding to requests for access to personal data made by the pupil or their parent or carer with parental responsibility.

13.1.1 There are two distinct rights of access to information held by schools about students, parents/carer and staff:

(a) Students and parents or those with Parental Responsibility have a right to make a request under the GDPR to access the personal information held about them.

(b) Students and parents or those with Parental Responsibility have a right to access the educational records. The right of those entitled to have access to curricular and educational records is defined within the Education (Pupil Information) (England) Regulations 2005.

13.2 Handling a subject access request for access to personal data:

13.2.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child.

For the purposes of a subject access request the school will apply the full legal definition of 'Parental Responsibility' when determining who can access a child's personal data.

13.2.2 Requests for information may come in from various sources whether verbally or in writing, which can include e-mail, to any member of staff. Where possible the requestor should be encouraged to complete the School's Subject Access Request form [Appendix B] to best capture what information is being requested and send the form to Mrs Torch. If the original request does not clearly identify the information required, then the school will seek further enquiries to clarify what information is being requested.

13.2.3 Requesters do not have to tell Mrs Torch their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.

A request is valid even if the individual has not sent it directly to the person who normally deals with such requests. So, it is important to ensure you recognise a subject access request (SAR) and forward it to the named person in school who will liaise with the school Data Protection Officer.

Any school employee who receives a request for a subject access request (SAR) must forward it immediately to Mrs Torch, no matter what form it is received in. Mrs Torch will log and acknowledge the request on the GDPRis portal to inform the school's DPO.

13.2.4. The identity of the requestor must be established before the disclosure of any information is made. Proof of the relationship with the child (if not known) must also be established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child.

Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence
- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement

13.2.5 No charge can be made for access to personal data that is not contained within an education record but the school reserves the right to cover its

communication costs e.g. photocopying, postage, in which case a fees notice will be sent to the requestor.

13.2.6 The response time for a subject access request is 1 calendar month from the date of receipt.

13.2.7 The relevant response time period for a subject access request will not commence until any necessary clarification of information has been sought and received from the requestor.

The time to respond can be extended to two months where the request is complex, when the volume of information is over 1,000 pages or when a number of third parties are included. Mrs Torch shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

13.2.8 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked Data Protection Policy May 2018 out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the school's legal obligations.

13.2.9 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

13.2.10 Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another person will be withheld along with any information that would reveal that the child is at risk of abuse, or information relating to Court Proceedings.

13.2.11 Where redaction has taken place then a full copy of the information provided will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the school's response to the request.

13.2.12 If there are concerns about the disclosure of information, additional advice will be sought.

13.2.13 The Data Protection Act currently sets out a number of exemptions which allow information to be withheld from data subjects in circumstances in which it would otherwise need to be disclosed. Current exemptions which are relevant include:

- Confidential references – schools do not have to provide subject access to references they have confidentially given in relation to an employee's employment;

- Management information – personal data which relates to management forecasting or planning is exempt from subject access (to the extent complying with the SAR would be likely to prejudice the business activity of the organisation);
- Legal advice and proceedings – schools do not have to disclose data which is covered by legal professional privilege;
- Settlement negotiations – the subject is not entitled to personal data which consists of a record of the employers' intentions in respect of settlement discussions that have taken place or are in the process of taking place with that individual.

13.3 Handling a request for access to a curricular and educational record as defined within the Education (Pupil Information) (England) Regulations 2005.

13.3.1 A parent may make a request to access information contained within their child's education record, regardless of whether the child agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the child.

13.3.2 For the purpose of responding to an Educational Records request, the School will apply the definition of 'parent' contained within the Education Act 1996.

13.3.3 An "educational record" means any record of information which-

(a) Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.

(b) Relates to any person who is or has been a pupil at any such school; and

(c) Originated from or was supplied by or on behalf of the persons specified in paragraph (a), other than information which is processed by a teacher solely for the teacher's own use

13.3.4 The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Education (Pupil Information) (England) Regulations 2005.

13.3.5 No charge will be made to view the education record.

13.3.6 The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days) or 1 calendar month, whichever is shorter.

13.4.7 An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the pupil or another person or if the disclosure of the information would reveal that the child is at risk of abuse.

14. Retention and Disposal of personal data

The Governing Body of the School will ensure that the school has a up to date and accurate retention and disposal schedule that is compliant with GDPR. The school will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule.

15. Security of personal data

15.1. The Security Principle

The Security Principle requires that appropriate security is put in place to prevent the personal data it holds being accidentally or deliberately compromised.

15.2 In order to comply with this principle the school will:

15.2.1 Ensure that all individuals involved in processing data understand the requirements of confidentiality, integrity and availability for the personal data being processed.

15.2.2 Undertake an analysis of the risks presented by its processing, and uses this to assess the appropriate level of security it needs to put in place to keep paper and electronic personal data secure and ensure that appropriate security measures are enforced

15.2.3 Ensure that only authorised individuals have access to personal data.

15.2.4 Put in place appropriate physical and organisational security measures, as well as technical measures, and regularly review the physical security of the school buildings and storage systems.

15.2.5 Require staff to ensure that no personal data will be left unattended in any vehicles and that if it is necessary to take personal data from school premises, for example to complete work from home, the data is suitably secured.

15.2.6 Review its information security policy regularly and takes steps to make sure the policy is implemented.

15.2.7 Put in place basic technical controls and be aware that it may also need to put other technical measures in place depending on the circumstances and the type of personal data it processes.

15.2.8 Use encryption and/or pseudonymisation where it is appropriate to do so.

15.2.9 Ensure that all portable electronic devices containing personal data are password protected.

15.2.10 Refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.

15.2.11 Make sure that it can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

15.2.12 Ensure that any data processor it uses also implements appropriate technical and organisational measures.

15.3. The school will conduct regular testing and reviews of its measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

16. Data breaches

16.1 A data breach may take many different forms:

(a) Loss or theft of data or equipment on which personal information is stored

(b) Unauthorised access to or use of personal information either by a member of staff or third party

(c) Loss of data resulting from an equipment or systems (including hardware or software) failure

(d) Human error, such as accidental deletion or alteration of data

(e) Unforeseen circumstances, such as a fire or flood

(f) Deliberate attacks on IT systems, such as cyber-attack, hacking, viruses or phishing scams

(g) Blagging offences where information is obtained by deceiving the organisation which holds it

16.2 Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher (or, in their absence, the Deputy Head Teacher), who will then inform the Data Protection Officer. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) will inform the Chair of Governors. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. The use of back-ups to restore lost/damaged/stolen data.

c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

16.3 Investigation

In most cases, the next stage would be for the DPO or Data Protection Lead (or nominated representative) to fully investigate the breach. The DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it (Appendix A). The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

16.4 Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach.

16.5 Review and Evaluation

Once the initial aftermath of the breach is over, the DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Leadership Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

16.6 Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

17. Complaints

17.1 Subject to paragraphs 17.2 and 17.3, complaints relating to the school's compliance with the GDPR will be dealt with in accordance with the school's Complaints Policy.

17.2 Complaints relating to access to personal information or access to education records should be made to the DPO (see section 4 of this policy) who will decide whether it is appropriate for the complaint to be dealt with through the school's complaints procedure. Complaints which are not appropriate to be dealt with through the school's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter.

17.3 Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453.

18. Consequences of a failure to comply

18.1 The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

18.2 Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

19. Links to other policies

This Policy should be read in conjunction with the following policies:

Freedom of Information Policy

Online Safety Policy

Records Retention and Disposal Policy

Keeping Children safe in Education 2022 and from September 2023 Keeping Children safe in Education 2023

Child protection and safeguarding policy 2022

Whistle Blowing policy 2018

20. Review

This policy will be reviewed every three years, or sooner if statutory requirements change.

21. Contacts

(a) Any enquiries in relation to this policy, should be directed to the Mr Adam via the School Office: enquiries@ursulinehigh.merton.sch.uk

(b) Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453

22. Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits automated decision-making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

Data Controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the GDPR. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in public authorities under the GDPR.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (not just action).

General Data Protection Regulation (GDPR): General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal data: Any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

Processing: Anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

School Day: Any day in which there is a session and pupils are in attendance.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

Working Days: Exclude school holidays and “inset” or training days where the pupils are not present.

23. Privacy Notices for Students

How We Use Your Information

Privacy Notice for Students

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.
We, Ursuline High School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is London Borough of Merton (see 'Contact us' below).

The personal data we hold
We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your test results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images
- Destinations

Why we use this data
We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in exams and work out whether you or your teachers need any extra help
- Track how well the school as a whole is performing
- Look after your wellbeing

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.
Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information
While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data
We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

We have a record retention schedule which sets out how long we must keep information about pupils. To request a copy please email Mrs Torch at enquiries@ursulinehigh.merton.sch.uk

Data sharing
We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- Our local authority – to meet our legal duties to share certain information with it, such as concerns about pupils' safety and exclusions
- The Department for Education (a government department)
- Your family and representatives
- Educators and examining bodies
- Our regulator (the organisation or "watchdog" that supervises us), ([specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – so that they can provide the services we have contracted them for
- Financial organisations

- Central and local government
- Our auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database
We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.
Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data.
You can also contact the Department for Education if you have any questions about the database.

Youth support services
Once you reach the age of 13, we are legally required to pass on certain information about you to The London Borough of Merton as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to The London Borough of Merton.

Transferring data internationally
Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights
How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.
You can make a complaint at any time by contacting our data protection officer.
You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

- Our Data Protection Officer: London Borough of Merton schoolsdpo@merton.gov.uk
- Our Data Protection Lead: Mr Adam enquiries@ursulinehigh.merton.sch.uk

24. Privacy Notices for Parents and Carers

How We Use Your Information

Privacy Notice for Parents and Carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **students**.

We, Ursuline High School, Crescent Road, Wimbledon, London, SW20 8HA, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Mr Adam (see 'Contact us' below).

The personal data we hold
Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school
- Destinations
- Primary School records

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data
We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care

- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data
We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.
Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information
While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.
Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How we store this data
We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school as instructed by the Government to comply with our legal obligations. Our record retention schedule/records management sets out how long we keep information about pupils.
A copy of our record retention schedule/records management policy can be obtained from Mrs Torch at enquiries@ursulinehigh.merton.sch.uk

Data sharing
We do not share information about pupils with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions

- The Department for Education to meet our legal obligations
- The pupil's family and representatives to support pupil progress, pastoral care and well-being
- Examining bodies to meet our legal obligation
- Our regulator – Ofsted to meet our legal obligation
- Suppliers and service providers – to enable them to provide the service we have contracted them for
- Central and local government to meet our legal obligation
- Our auditors to meet our legal obligation
- Survey and research organisations to support learning and pastoral work
- Health authorities to support well-being of pupils
- Security organisations to support pupil well-being and safeguarding
- Health and social welfare organisations to support pupil safeguarding
- Professional advisers and consultants to support pupils progress and well-being
- Charities and voluntary organisations to support pupils learning
- Police forces, courts, tribunals to support pupils well-being and legal obligations
- Professional bodies to support pupil progress and well-being

National Pupil Database
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.
You can also contact the Department for Education with any further questions about the NPD.

Youth support services
Once our pupils reach the age of 13, we are legally required to pass on certain information about them to the London Borough of Merton, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the London Borough of Merton.

Transferring data internationally
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.

Parents and pupils' rights regarding personal data
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

Parents/carers have a legal right to access to their child's **educational record**. To request access, please contact Mrs Torch, Headteacher's PA at enquiries@ursulinehigh.merton.sch.uk

Other rights
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing

- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

- Our Data Protection Officer: London Borough of Merton schoolsdpo@merton.gov.uk
- Our Data Protection Lead: Mr Adam enquiries@ursulinehigh.merton.sch.uk

25. Privacy Notices for the School Workforce

How We Use Your Information

Privacy Notice for School Workforce

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.
We, Ursuline High School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is London Borough of Merton (see 'Contact us' below).

The personal data we hold
We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and application form or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary, low-level concerns and/or grievance procedures
- Absence data
- Copy of driving licence/passport (identity)
- Photographs
- CCTV footage
- Data about your use of the school's information and communications system
- DBS
- CPD Record
- Agreements with School Policies e.g., Professional Conduct

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs and disability
- Health, including any medical conditions, and sickness records

Why we use this data
The purpose of processing this data is to help us run the school, including to:
- Enable you to be paid
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body
- Supply Census data to DfE and the Catholic Education Service

Our lawful basis for using this data

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:
- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:
- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)
- We have legitimate interests in processing the data – for example, where:

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.
Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information
While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.
Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data
We create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with us has ended, we will retain this file and delete the information in it in accordance with our record retention schedule. To request a copy please email Mrs Torch at enquiries@ursulinehigh.merton.sch.uk

Data sharing
We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.
Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and [maintained schools only] information about headteacher performance and staff dismissals*
- *The Department for Education for Census requests*
- *Examining bodies as legally required*
- *Our regulator - Ofsted as legally required*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll*
- *Financial organisations – to meet our financial obligations*
- *Central and local government for HR purposes*
- *Our auditors – to meet our financial obligations*
- *Security organisations as legally required*
- *Health and social welfare organisations for staff well-being*
- *Police forces, courts, tribunals as legally required*

Transferring data internationally
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.

Your rights
How to access personal information we hold about you
Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.
If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints
We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact:

- Our Data Protection Officer: London Borough of Merton schoolsdpo@merton.gov.uk
- Our Data Protection Lead: Mr Adam enquiries@ursulinehigh.merton.sch.uk

Appendix A

Data Breach Reporting Form

	Report prepared by: **Date:** **On behalf of:**	Ursuline High School
1	**Summary of the event and circumstances:**	
2	**Type and amount of data** **(personal/staff, student, parental/carer):**	
3	**Actions taken to retrieve the information and minimise the effect of the breach:**	
4	**Details of notification to affected data subject:** **(if applicable)** **Has a complaint been received from the affected data subject?**	
5	**Breach of procedure / policy by staff member:**	
6	**Details of Data Protection training provided/taken:**	
7	**Any procedure changes required to reduce risks of future data loss:**	

Appendix B

Form for Submitting Subject Access Requests

Ursuline High School Date:

Re: Subject Access Request

Dear Mrs Torch,

Please provide me with the information about me that I am entitled to under the Data Protection Act 2018 and General Data Protection Regulation (UK GDPR). This is so I can be aware of the information you are processing about me, and verify the lawfulness of the processing.

Here is the necessary information:

Name	
Relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *Your personnel file* • *Your child's medical records* • *Your child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.

Please bear in mind that under the UK GDPR you cannot charge a fee to provide this information, and in most cases, must supply me with the information within one month.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,