University of Birmingham School

Data Protection Policy

March 2025

University of Birmingham School
Data Protection Policy

Review Frequency	Annually	**Review date**	March 2025
Governing Committee Responsible	Resources Committee	**Next Due**	March 2026
Governor Approval date	12 March 2025	**Website**	Yes
Employees Responsible	C Townsend	**Date Produced**	

Contents	**Page**

At University of Birmingham School we refer to **Pupils** (who are in Years 7-11 and aged 11-16) and **Students** (who are in Years 12/ 13 and aged 17-18)

1. Aims

Our School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

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:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2020
- https://www.gov.uk/data-protection (the Data Protection Act 2018).

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

TERM	DEFINITION
Personal data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category 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 will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

TERM	DEFINITION
Special Category Data and Data Relating to Criminal Convictions and Offences	Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical and mental health, sexuality and biometric or genetic data. Personal data relating to criminal offences and convictions is included here for the purposes of this policy. This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.
Data subject	An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.
Data controller	The organisation storing and controlling such information (i.e., the School) is referred to as the Data Controller.
Processing	Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
Pseudonymised	The process by which personal data is processed in such a way that that it cannot be used to identify an individual without the use of additional data, which is kept separately and subject to technical and organisational measures to ensure that the personal data cannot be attributed to an identifiable individual.

4. The data controller

Our School processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller.

The School has paid its data protection fee to the ICO, as 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 Governing board

The governing board has overall responsibility for ensuring that our School complies with all relevant data protection obligations.

5.2 Data protection officer (DPO)

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

The DPO is responsible for overseeing this Data Protection Policy and developing data-related policies and guidelines. Please contact the DPO with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

- If you are unsure of the lawful basis being relied on by the School to process personal data;
- If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- If you need to draft privacy notices or fair processing notices;
- If you are unsure about the retention periods for the personal data being processed :
- If you are unsure about what security measures need to be put in place to protect personal data;
- If there has been a personal data breach;
- If you are unsure on what basis to transfer personal data outside the EEA;
- If you need any assistance dealing with any rights invoked by a data subject;
- Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- If you plan to undertake any activities involving automated processing or automated decision making;
- If you need help complying with applicable law when carrying out direct marketing activities;
- If you need help with any contracts or other areas in relation to sharing personal data with third parties.

5.3 Director of information & Systems

The Director of Information & Systems acts as the representative of the data controller on a day-to-day basis.

5.4 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 DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - 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 UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6 Data protection principles

The School are responsible for and adhere to the principles relating to the processing of personal data as set out in the UK GDPR. The principles the School must adhere to are set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The School only collect, process and share personal data fairly and lawfully and for specified purposes.
The School must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.
Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e., that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following fair processing conditions are met: -
The data subject has given their consent;
The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
To protect the data subject's vital interests;
To meet our legal compliance obligations (other than a contractual obligation);
To perform a task in the public interest or in order to carry out official functions as authorised by law;
For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -
The data subject has given their explicit consent;
The processing is necessary for the purposes of exercising or performing any right or obligation that is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
To protect the data subject's vital interests;
The processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity
Where the data has been made public by the data subject;
To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
Where it is necessary for reasons of public interest in the area of public health;
The processing is necessary for archiving, statistical or research purposes.
The School identifies and documents the legal grounds being relied upon for each processing activity.

Criminal Record Data

Criminal records data is processed, also identify a lawful condition for processing that data and document it.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.
Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which

they signify agreement to the processing of personal data relating to them. Explicit consent is needed in cases of processing special category data and requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).
A data subject will have consented to processing of their non-special category personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.
Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.
In cases of processing special category data and explicit consent, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.
The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes
Personal data will not be processed in any manner that is incompatible with the legitimate purposes specified.
The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
The School will only process personal data when our obligations and duties require us to. We will not collect excessive data and will ensure any personal data collected is adequate and relevant for the intended purposes.
When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. Please refer to Appendix 2

Principle 4: Personal data must be accurate and, where necessary, kept up to date
The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.
Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form that permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.
We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.
Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
In order to ensure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as: -
Encryption;
Pseudonymisation (this is where the School replaces 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);
Ensuring authorised access on both hard copy and electronic files (i.e. that only people who have a need to know the personal data are authorised to access it);

Adhering to confidentiality principles;
Ensuring personal data is accurate and suitable for the process for which it is processed.
The School follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.
The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

Sharing Personal Data
The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:
Whether the third party has a need to know the information for the purposes of providing the contracted services;
Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
Whether the transfer complies with any applicable cross border transfer restrictions; and
Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.
There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data outside the European Economic Area (EEA)
The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.
The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data outside the UK
The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have 1 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the School (where the processing is not for any tasks the

School performs as a public authority) 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 1 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 defense 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.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

This will be done in accordance with the School's record retention schedule.

8. Sharing personal data

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, Ofsted or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of the School shall be clearly defined within written notifications including details and the basis for sharing the data.

Transfer of Data outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Transfer of Data outside the UK

The School may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

Please refer to Appendix 3 for guidance on how data subject access requests should be handled.

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 aged 12 and above are generally 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 not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 School days of receipt of a written request.

If the request is for a copy of the educational record, the School may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive School dinners instead of paying with cash, we will comply with the requirements of the Protection of Freedoms Act 2012,

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The School will get written consent from at least 1 parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the School's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for School dinners via debit card / contactless at each transaction if they wish.

Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the School's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the School will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the School site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to a member of the Senior Leadership Team in the first instance.

13. Photographs and videos

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

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

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

Any photographs and videos taken by parents/carers at School events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the School takes photographs and videos, 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. Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chat-bots such as ChatGPT and Google Bard. University of Birmingham School recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chat-bots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, University of Birmingham School will treat this as a data breach, and will follow the personal data breach procedure outlined in Appendix 1.

15. 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:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- 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 data protection 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 (the DPO will advise on this process)
- 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School and DPO, and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

16. 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 staffroom tables, 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 10 characters long containing letters and numbers are used to access School computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for School-owned equipment (see our Acceptable Use of ICT Policy)
- 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)

17. 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.

18. 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 after becoming aware of it. Such breaches in a School context may include, but are not limited to:

- A non-anonymised dataset being published on the School website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a School laptop containing non-encrypted personal data about pupils

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person designated as the key point of contact for personal data breaches (Director of Information & Systems) or your DPO.

19. Training

All staff and governors 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.

20. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

21. Links with other policies

This data protection policy is linked to the School's:

- Freedom of information Policy
- CCTV Policy
- Acceptable Use of ICT Policy
- Safeguarding Policy
- Media Consent Policy

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing them at dataservice@judicium.com
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the Principal / Director of Information & Systems and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types at the end of this procedure)
- The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
- The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Shared Drive.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the School's awareness of the breach. As required, the DPO will set out:
    - 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
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - 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 DPO will report as much as they can within 72 hours of the School's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- Where the School is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - 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
- The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - 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 on the Shared Drive
- The DPO and Principal / Director of Information & Systems will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and Principal / Director of Information & Systems will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the School to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT Network Manager to attempt to recall it from external recipients and remove it from the School's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO 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

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the School should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the School website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A School laptop containing non-encrypted sensitive personal data being stolen or hacked
- The School's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix2 – Data Retention Guidance

The below table provides guidance for how long records should be retained.

Basic file description	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative Life of the record
Child Protection			
Child Protection files	Education Act 2012, s175, related guidance "Keeping Children Safe in Education"	DOB+ 25 years	SECURE DISPOSAL
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL
Governors			
Minutes - Principal set (signed)		Permanent	Retain in School for 6 years from date of meeting
Minutes- Inspection copies		Date of meeting+ 3 years	SECUREDISPOSAL [If these minutes contain any sensitive personal information they Should be shredded]
Agendas		Date of meeting	SECUREDISPOSAL
Reports		Date of report + 6 years	Retain in School for 6 years from date of meeting

Instruments of Government		Permanent	Retain in School whilst School is open
Trusts and Endowments		Permanent	Retain in School whilst operationally required
Action Plans		Date of action plan+ 3 years	SECUREDISPOSAL
Policy documents		Expiry of policy	Retain in School whilst policy is operational (this includes if the expired policy is part of a past decision making process)
Complaints files		Date of resolution of complaint + 6 years	Retain in School for the first six years. Review for further retention in the case of contentious disputes SECURE DISPOSAL routine complaints
Annual Reports required by the Department for Education	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
Management			
Logbooks		Date of last entry in the book + 6 years	Retain in the School for 6 years from the date of the last entry
Minutes of the Senior Management Team and other internal administrative bodies		Date of meeting+ 5 years	Retain in the Schoolfor5 years from meeting
Reports made by the Principal or the Senior Leadership Team		Date of report + 3 years	Retain in the School for 3 years from meeting
Records Principal, Senior and Middle Leaders another members of staff with administrative responsibilities		Closure of file + 6 years	SECUREDISPOSAL

Correspondence created by Principal, Senior and Middle Leaders and other members of staff with administrative responsibilities		Date of correspondence+ 3 years	SECUREDISPOSAL
Professional Development Plans		Closure+ 6 years	SECUREDISPOSAL
School Development Plans		Closure+ 6 years	Review
Admissions- if the admission is Yes Successful		Admission+ 1 year	SECUREDISPOSAL
Admissions- if the appeal is Yes Unsuccessful		Resolution of case+ 1 year	SECUREDISPOSAL
Admissions- Secondary Schools - Casual		Current year+ 1 year	SECUREDISPOSAL
Proofs of address supplied by parents as part of the admissions process		Current year+ 1 year	SECUREDISPOSAL
Pupils			
Admission Registers		Date of last entry in the book (or file) + 6 years Re considers Retention Period. Feedback from Teaching Relative was thought to be 7 Year Retention. These records are no longer generated in paper but Electronically held using Arbor (MIS) software.	Retain in the School for 6 years from the date of the last entry then consider transfer to the Archives
Attendance registers		Date of register+ 3 years	SECUREDISPOSAL [If these records are retained electronically any backup copies

			Should be destroyed at the same time]
Pupil Files Retained in Schools	Limitation Act 1980	DOB of the pupil + 25 years	SECUREDISPOSAL
Pupil Files	Limitation Act 1980	DOB of the pupil + 25 years	SECUREDISPOSAL
Special Educational Needs Files, reviews and Individual Education Plans		DOB of the pupil + 25 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to Keep the records longer than the minimum retention period.	SECUREDISPOSAL
Correspondence Relating to Authorized Absence and Issues		Date of absence+ 2 years	SECUREDISPOSAL
Examination results – Public		Year of examinations+ 6 years	SECUREDISPOSAL
Examination results – Internal		Current year+ 5 years	SECUREDISPOSAL
Any other records created in the course of contact with pupils		Current year+ 3 years	Review at the end of 3 years and either allocate a further retention Period or SECURE DISPOSAL
Statement maintained under The Education Act 1996 - Section 324	Special Educational Needs and Disability Act 2001 Section 1	DOB+ 30 years	SECURE DISPOSAL unless legal action is pending
Proposed statement or amended statement	Special Educational Needs and Disability Act 2001 Section 1	DOB+ 30 years	SECUREDISPOSAL unless legal action is pending

Advice and information to parents regarding educational needs	Special Educational Needs and Disability Act 2001 Section 1	Closure+ 12 years	SECURE DISPOSAL unless legal action is pending
Accessibility Strategy	Special Educational Needs and Disability Act 2001 Section 1	Closure+ 12 years	SECURE DISPOSAL unless legal action is pending
Parental permission slips for School trips- where there has been no major incident		Conclusion of the trip	SECUREDISPOSAL
Parental permission slips for School trips - where there has been a major incident.	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECUREDISPOSAL
Records created by Schools to obtain approval to run an Educational Visit outside the Classroom	3 part supplement to the Health& Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	SECUREDISPOSAL
Walking Bus registers		Date of register+ 3 years This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of Time required for accident reporting	SECUREDISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]
Curriculum			
School Development Plan		Current year+ 6 years	SECUREDISPOSAL
Curriculum returns		Current year+ 3 years	SECUREDISPOSAL
Schemes of work		Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL

Timetable		Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Class record books		Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Mark Books		Current year+ 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Record of homework set		Current year+ 1 year	It may be appropriate to review These records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Pupils' work		Current year+ 1 year	It may be appropriate to review These records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Examination results		Current year+ 6 years	SECUREDISPOSAL
SATS records- Examination Papers and Results		Current year+ 6 years	SECUREDISPOSAL
PAN reports		Current year+ 6 years	SECUREDISPOSAL
Value Added& Contextual Data		Current year+ 6 years	SECUREDISPOSAL
Self-Evaluation forms		Current year+ 6 years	SECUREDISPOSAL
Personnel Records held in Schools			
Timesheets, sick pay	Financial Regulations	Current year+ 6 years	SECUREDISPOSAL
Staff Personal files		Termination+ 7 years	SECUREDISPOSAL
Interview notes and recruitment records		Date of interview+ 6 months	SECUREDISPOSAL
Pre-employment vetting information (including DBS	DBS guidelines	Date of check + 6 months	SECUREDISPOSAL

checks)			
Disciplinary proceedings: oral warning	Where the warning relates to child Protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning+ 6 months	SECUREDISPOSAL
Disciplinary proceedings: written warning	Where the warning relates to child Protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning+ 6 months	SECUREDISPOSAL
Disciplinary proceedings: final written warning	Where the warning relates to child Protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	Date of warning+ 12 months	SECUREDISPOSAL
Disciplinary proceedings: case not found	Where the warning relates to child Protection issues see Child Protection. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.	If child protection related please see child protection, otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECUREDISPOSAL
Records relating to accident/ injury at work		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied	SECUREDISPOSAL

Annual Appraisal and Assessment Records		Current year+ 5 years	SECUREDISPOSAL
Salary cards		Last date of employment + 85 years	SECUREDISPOSAL
Maternity pay records	Statutory Maternity Pay(General) Current year +3yrs Regulations 1986 (SI 1986/ 1960), revised1999 (SI 1999/ 567)	Current year+3yrs	SECUREDISPOSAL
Records held under Retirement benefits Schemes (Information Powers) Regulations1995		Current year+ 6 years	SECUREDISPOSAL
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure		Where possible these should be Checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then This should be placed on the Member of staff's personal file.	SECUREDISPOSAL
Health and Safety			
Accessibility Plans		Current year+ 6 years	SECUREDISPOSAL
Accident Reporting– Adults		Date of incident + 7 years	SECUREDISPOSAL
Accident Reporting- Children		DOB of child+ 25 years	SECUREDISPOSAL
COSHH		Current year + 10 years [where appropriate an additional retention period may be allocated]	SECUREDISPOSAL
Incident reports		Current year+ 20 years	SECUREDISPOSAL
Policy Statements		Date of expiry+ 1 year	SECUREDISPOSAL
Risk Assessments		Current year+ 3 years	SECUREDISPOSAL
Process of monitoring of areas where employees and persons are		Last action+ 40 years	SECUREDISPOSAL

likely to have become in contact with asbestos			
Process of monitoring of areas where Employees and persons are likely to have come in contact with radiation		Last action+ 50 years	SECUREDISPOSAL
Fire Precautions log books		Current year+ 6 years	SECUREDISPOSAL
Administrative			
Employer's Liability certificate		Closure of the School + 40 years	SECUREDISPOSAL
Inventories of equipment & furniture		Current year+ 6 years	SECUREDISPOSAL
General file series		Current year+ 5 years	Review to see whether a further retention period is required
School brochure or prospectus		Current year+ 3 years	Review to see whether a further retention period is required
Circulars(staff/ parents/ pupils)		Current year+ 1 year	SECUREDISPOSAL
Newsletters, ephemera		Current year+ 1 year	Review to see whether a further retention period is required
Visitors book		Current year+ 2 years	Review to see whether a further retention period is required
PTA/ Old Pupils Associations		Current year+ 6 years	Review to see whether a further retention period is required
Finance			
Annual Accounts	Financial Regulations	Current year+ 6 years	
Loans and grants	Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further Retention period is required
Contracts - underseal		Contract completion date + 12 years	SECUREDISPOSAL
Contracts – under signature		Contract completion date+ 6 years	SECUREDISPOSAL
Contracts – monitoring records		Current year+ 2 years	SECUREDISPOSAL
Copy orders		Current year+ 2 years	SECUREDISPOSAL

Budget reports, budget monitoring etc.		Current year+ 3 years	SECUREDISPOSAL
Invoice, receipts and other records covered by the Financial Regulations	Financial Regulations	Current year+ 6 years	SECUREDISPOSAL
Annual Budget and background papers		Current year+ 6 years	SECUREDISPOSAL
Order books and requisitions		Current year+ 6 years	SECUREDISPOSAL
Delivery Documentation		Current year+ 6 years	SECUREDISPOSAL
Debtors' Records	Limitation Act 1980	Current year+ 6 years	SECUREDISPOSAL
School Fund- Cheque books		Current year + 3 years	SECUREDISPOSAL
School Fund- Paying in books		Current year+ 6 years then review	SECUREDISPOSAL
School Fund- Ledger		Current year + 6 years then review	SECUREDISPOSAL
School Fund- Invoices		Current year + 6 years then review	SECUREDISPOSAL
School Fund- Receipts		Current year+ 6 years	SECUREDISPOSAL
School Fund- Bank statements		Current year + 6 years then review	SECUREDISPOSAL
School Fund- School Journey books		Current year + 6 years then review	SECUREDISPOSAL
Student grant applications		Current year+ 3 years	SECUREDISPOSAL
Free School meal registers		Current year+ 6 years	SECUREDISPOSAL
Petty cash books		Current year+ 6 years	SECUREDISPOSAL
Property			
Title Deeds		Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
Plans		Permanent	Retain in School whilst operational
Maintenance and contractors	Financial Regulations	Current year+ 6 years	SECUREDISPOSAL
Leases		Expiry of lease+ 6 years	SECUREDISPOSAL
Lettings		Current year+ 3 years	SECUREDISPOSAL

Burglary, theft and vandalism report forms		Current year+ 6 years	SECUREDISPOSAL
Maintenance log books		Current year+ 6 years	SECUREDISPOSAL
Contractors' Reports		Current year+ 6 years	SECUREDISPOSAL
Department for Education			
OFSTED reports and papers		Replace former report with any new inspection report	Review to see whether a further retention period is required
Returns		Current year+ 6 years	SECUREDISPOSAL
Schools Meals			
Dinner Register		Current year+ 3 years	SECUREDISPOSAL
School Meals Summary Sheets		Current year+ 3 years	SECUREDISPOSAL

Appendix 3 – Subject Access Requests (SARs)

Under Data Protection Law, data subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of and verify the lawfulness of the processing of personal data that the School are undertaking. It is designed to assist individuals in understanding how and why we are using their data and to check that we are doing so lawfully. The main provisions are to be found in Articles 12 and 15 of the UK GDPR and Section 45 of the Data Protection Act 2018.

This appendix provides guidance for staff members on how data subject access requests should be handled and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the School at potentially significant risk and so the School takes compliance with this policy very seriously.

A data subject has the right to be informed by the School of the following: -

a) Confirmation that their data is being processed;

b) Access to their personal data;

c) A description of the information that is being processed;

d) The purpose for which the information is being processed;

e) The recipients/class of recipients to whom that information is or may be disclosed;

f) Details of the School's sources of information obtained;

g) In relation to any personal data processed for the purposes of evaluating matters in relation to the data subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and

h) Other supplementary information.

Dealing with a SAR is time critical and must be prioritised. Other than in exceptional cases, we will have only one month in which to respond to a SAR and even if an extension of the time limit is permitted, the individual must still be informed within that month of the fact that the request will take longer to process and the reasons for the delay. Failure to deal with a SAR within that period could leave us open to the possibility of being fined by the ICO.

All staff must be aware of the potential for receiving a SAR and the importance of dealing with such as request as a matter of urgency.

Anyone within the School may receive a SAR. It does not need to be made to a nominated person or even to a person responsible for dealing with either the data subject or information of that type. It will be equally as valid if sent to anyone within the school.

If you receive a SAR, please contact the Director of Information and Systems. A request for information does not need to mention that it is a SAR provided that it is clear that it is an individual asking for their own personal data. There is no specified wording and it does not have to be on an official form. A SAR does not

need to be in writing and can be made verbally, by post, by email or even using social media where relevant.

How to Recognise a Subject Access Request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text, social media) or verbally (e.g., during a telephone conversation or meeting). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' would constitute a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data and not information relating to other people.

How to Make a Data Subject Access Request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

If a request is made verbally, we will ensure we follow this up with something in writing to confirm what has been requested and outline the timeframe for dealing with the request.

What to do When You Receive a Data Subject Access Request

All data subject access requests should be immediately directed to the Director of Information and Systems who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the School must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual.

Acknowledging the Request

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information if it is not clear what information is required;

- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or

- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

Verifying the Identity of a Requester or Requesting Clarification of the Request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

When it is necessary to verify the identity of the person making the request, the one calendar month period for responding begins when sufficient confirmation of identity is provided.

When it is necessary to request more information for the purpose of clarifying the request, the one calendar month period for responding pauses when further information is requested and does not restart until sufficient clarification is provided.

In both cases, the school will be unable to comply with the request if they do not receive the additional information.

Requests Made by Third Parties or on Behalf of Children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example, if it is likely to cause detriment to the child.

Fee For Responding to a SAR

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the School will inform the requester why this is considered to be the case and that the School will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the School is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity and in the case of a third party requester, the written authorisation of the data subject has been received. Where the school may be required to get consent from a pupil, the time period will not start until consent is received.

The period for response may be extended by a further two calendar months in relation to complex requests.

What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School Closure Periods

The school may not be able to respond to requests received during or just before school closure periods within the one calendar month response period. This is because the staff required to process your request may not be available. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request). However, if we can acknowledge the request, we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be Provided in Response to a Request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data;
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing;
    - to lodge a complaint with the ICO;
    - where the personal data has not been collected from the individual, any information available regarding the source of the data;
    - any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in

which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

Therefore, the School is allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

How to Locate Information

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the School may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV;
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data;
- data systems held externally by our data processors;
- safeguarding systems (such as Safeguard My School);
- MIS system (such as Arbor);
- occupational health records;
- pensions data;
- share scheme information;
- insurance benefit information.

The School should search these systems using the individual's name, initials, employee number or other personal identifier as a search determinant.

Protection of Third Parties - Exemptions to the Right of Subject Access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or

- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

Other Exemptions to the Right of Subject Access

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which is subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in

relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

Refusing to Respond to a Request

The school can refuse to comply with a request if the request in certain circumstances. These include:

- Where the SAR is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;
- To avoid obstructing an official or legal inquiry, investigation or procedure;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security;
- To protect the rights and freedoms of others.

In the event that you have concerns about supplying the information, you must always refer the matter to DPO who will make the decision on our behalf.

In the event that we decide not to comply with the SAR, then the data subject must be informed, without undue delay (and in all cases within one month of receipt of the request), of:

- The reasons we are not taking action;
- That they have a right to make a complaint to the ICO or another supervisory authority; and
- That they are entitled to seek to enforce their right through a judicial remedy.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record Keeping

A record of all subject access requests shall be kept by the Director of Information and Systems. The record shall include the date the SAR was received, the name of the requester, what data the School sent to the requester and the date of the response.

Appendix A – Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of Identity

We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

Birth certificate
Driving license
Passport
An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

Birth certificate
Driving license
Passport
An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

Letter of authority
Lasting or Enduring Power of Attorney
Evidence of parental responsibility
Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

Receive the information by post*
Receive the information by email
Collect the information in person
View a copy of the information only
Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: d.lowy@uobschool.org.uk