



# **GUISELEY SCHOOL**

## Data Protection Policy

Approved on:	15 May 2018
Reviewed on:	27 February 2024
Next Review:	Spring term 2025
Governors' Committee:	Personnel
Responsible Officer:	DPC

# Contents

Data Protection Policy.....	1
1. Aims .....	3
2. Legislation and guidance.....	3
3. Definitions.....	4
4. The data controller.....	5
5. Roles and responsibilities.....	5
6. Data protection principles.....	7
7. Collecting personal data .....	7
8. Sharing personal data .....	8
9. Subject access requests and other rights of individuals .....	9
10. Consent .....	12
11. Parental requests to see the educational record.....	13
12. Biometric recognition systems.....	13
13. CCTV.....	14
14. Photographs and videos .....	14
15. Data protection by design and default .....	14
16. Data security and storage of records .....	15
17. Disposal of records.....	16
18. Personal data breaches.....	16
19. Breach notification data controller to data subject .....	16
20. Training.....	17
21. Monitoring arrangements.....	17
22. Links with other policies .....	17
Appendix I: Personal data breach procedure .....	18
Appendix II: Acceptable Use / Bring Your Own Device Considerations .....	21
Appendix III: Consent Form .....	22
Appendix IV: Withdrawal of Consent Form (Pupil) .....	27
Appendix V: Withdrawal of Consent Form (Adult) .....	28
Appendix VI: Biometric Consent.....	29
Appendix VII: Subject Access Request Form.....	30
Appendix VIII: Complaints form.....	32

## 1. Aims

Our school is committed to working effectively to provide a secure environment to protect data about staff, students, parents, governors, visitors and other individuals that we collect, store and process in accordance with the [General Data Protection Regulation \(UK GDPR\)](#) and the provisions of the Data Protection Act 2018 (DPA 2018). Whilst there is a statutory duty that is important, the fact that we store data about individuals means that we are responsible for that data and we take that very seriously. This policy, and the Privacy Notices, sets out how we look after and use data.

The General Data Protection Regulation (UK GDPR) is a European Directive that was brought into UK law with an updated Data Protection Act in May 2018. It was brought into line with changes to the UK leaving the Eu on 31 December 2020.

The UK GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The UK GDPR exists to protect individual rights in an increasingly digital world.

The UK GDPR applies to everyone, including schools. As Public Bodies schools have more obligations than some small businesses. It is mandatory to comply with the UK GDPR and proposed provisions in the new Act and as such want to make sure information about students, parents, staff and volunteers is kept secure and within the 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 GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [UK GDPR](#) and the ICO's [codes of practice](#).

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 \(Student Information\) \(England\) Regulations 2005](#), which gives parents the right of access to their child's educational record.

### 3. Definitions

Term	Definition
<p><b>Personal data</b></p>	<p>Any information relating to an identified, or identifiable, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> <li>• Name (including initials)</li> <li>• Identification number</li> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity and can include opinions.</p>
<p><b>Special categories of personal data</b></p>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<p><b>Processing</b></p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<p><b>Data subject</b></p>	<p>The identified or identifiable individual whose personal data is held or processed.</p>

<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data. Our school governing body is the data controller. They have ultimate responsibility for how school manages data. They delegate this to data processors to act on their behalf.
<b>Data processor</b>	<p>This is a person or organisation that uses, collects, accesses or amends the data that the controller has collected or authorised to be collected. It can be a member of staff, a third- party company, possibly a governor, a contractor or temporary employee. It can also be another organisation such as the police or the LA.</p> <p>Data controllers must make sure that data processors are as careful about the data as the controller themselves. The UK GDPR places</p>
	additional obligations on organisations to make sure that Data Controllers require contractual agreements to ensure that this is the case.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

## 4. The Data Controller

Our school processes personal data relating to parents, students, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

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

### 5.1 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

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

Within school the **Data Compliance Officer** is the first point of contact for individuals whose data the school processes, and they will liaise directly with the DPO, who is also the point of contact with the Information Commission Officer (ICO).

Full details of the DPO's responsibilities are set out in the school's contract with them.

### Data Compliance Officer in School

#### Andrew Mathieson

IT Services Lead  
Guiseley School  
Fieldhead Road  
Guiseley  
LS20 8DT  
Email: [info@guiseleyschool.org.uk](mailto:info@guiseleyschool.org.uk)

### Data Protection Officer

#### John Walker

JA Walker Solicitor  
Office 7, The Courtyard  
Gaulby Lane  
Stoughton  
LE2 2FL  
[info@jawalker.co.uk](mailto:info@jawalker.co.uk)

## 5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis and delegates responsibility to the Data Compliance Officer (DCO) in school.

## 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 DCO in the first instance and then the DPO if required 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 European Economic Area
- 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 UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
4. Accurate and, where necessary, kept up to date
5. Kept for no longer than is necessary for the purposes for which it is processed
6. Processed in a way that ensures it is appropriately secure

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

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

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

- 7.1.1** 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**
- 7.1.2** The data needs to be processed so that the school can **comply with a legal obligation**
- 7.1.3** The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- 7.1.4** The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- 7.1.5** The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- 7.1.6** The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the UK GDPR and Data Protection Act 2018.

If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

## **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.

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 records management procedures which follows the Information and Records Management Society's toolkit for schools which can be found in the Staff GDPR folder on the VLE.

## **8. Sharing personal data**

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

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders



- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## 9. Subject access requests and other rights of individuals

### 9.1 Subject access requests

As an organisation we collect and process data about individuals. We explain what information we collect, and why in our Privacy Notices.

Any individual, or person with parental responsibility, or young person with sufficient capacity to make a request is entitled to ask what information is held. Copies of the information shall also be made available on request. A form to complete is available and the party making the request must provide identification evidence in order to process the request.

The information will be provided in an electronic format, within one calendar month of the request. However, in some circumstances this can be extended if the request is complicated or the data cannot be accessed. The maximum extension is up to two months.

To collate and manage requests we have designated the School's Data Compliance Officer, Andrew Mathieson, to co-ordinate all requests. Please ensure that requests are made on the Subject Access request form (see [Appendix VII](#)) and are submitted to the school office or by email to [info@guiseleyschool.org.uk](mailto:info@guiseleyschool.org.uk) and clearly marked for her attention.

If staff receive a subject access request they must immediately forward it to the DCO (Andrew Mathieson / DPO John walker).

Evidence of their identity, on the basis of the information set out and the signature on the identity must be cross-checked to that on the application form. Discretion about employees and persons known to the school may be applicable but if ID evidence is not required an explanation must be provided by school staff and signed and dated accordingly.

Exemptions to a SAR exist and may include:

- Education, Health, Social Work records

- Examination marks and scripts
- Safeguarding records
- Special educational needs
- Parental records and reports
- Legal advice and proceedings
- Adoption and Court records and/or reports
- Regulatory activity and official requests e.g. DfE statistical information
- National security, Crime and taxation
- Journalism, literature and art
- Research history, and statistics
- Confidential references All data subjects have the right to know:
  - What information is held?
  - Who holds it?
  - Why is it held?
  - What is the retention periods?

That each data subject has rights. Consent can be withdrawn at any time (to some things)  
They also have a right:

- To request rectification, erasure or to limit or stop processing
- To complain

Many of these questions will be within the Privacy Notices on the [website](#).

## 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 students at our school may not be granted without the express permission of the student. This is not a rule and a student'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 two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge

- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary. We will not disclose information if it:
- Might cause serious harm to the physical or mental health of the student or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

#### **9.4 Complaints & the Information Commissioner Office (ICO)**

The School's Complaints Policy, which is available from the School's [website](#), deals with complaints about Data protection issues.

There is a right to complain if you feel that data has been shared without consent or lawful authority.

You can complain if you have asked us to erase, rectify, not process data and we have not agreed to your request.

We will always try to resolve issues on an informal basis, and then through our formal complaints procedure. Please complete the complaints form (see [appendix VIII](#)), and we will contact you with more details about the timescale and process.

In the UK it is the ICO who has responsibility for safeguarding and enforcing the DPA obligations. Email: [casework@ico.org.uk](mailto:casework@ico.org.uk) Helpline: 0303 123 1113 web: [www.ico.org.uk](http://www.ico.org.uk)

#### **9.5 Other data protection rights of the individual**

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)

- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

## 10. Consent

As a school we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required.

However, in most cases data will only be processed if explicit consent has been obtained.

Consent is defined by the UK GDPR as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

### 10.1 Consent and Renewal

On the school website we have ‘Privacy Notices’ that explain how data is collected and used. It is important to read those notices as it explains how data is used in detail.

Obtaining clear consent and ensuring that the consent remains in place is important for school. We also want to ensure the accuracy of that information.

### 10.2 For Students and Parents/Carers

On arrival at school you will be asked to complete a form giving next of kin details, emergency contact and other essential information. We will also ask you to give consent to use the information for other in school purposes, as set out on the data collection/consent form (see [Appendix III](#)).

We review the contact and consent form on an annual basis. It is important to inform school if details or your decision about consent changes. A **consent form** is also available from the school office.

### 10.3 Student consent procedure

Where processing relates to a child under 16 years old, school will obtain the consent from a person who has parental responsibility for the child.

Students may be asked to give consent or to be consulted about how their data is obtained, shared and used in certain situations.

### 10.4 Withdrawal of Consent

Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent the school will consider each situation on the merits and within the principles of UK GDPR and also child welfare, protection and safeguarding principles.

Please complete the appropriate **withdrawal of consent form** for staff/student (see [Appendix IV](#) and [Appendix V](#)).

## 11. 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 student) within 15 school days of receipt of a written request.

## 12. Biometric recognition systems

Guiseley School uses students' biometric data as part of an automated biometric recognition system for our cashless catering system and confirm that in its use 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 one parent or carer before we take any biometric data from their child and first process it (see the Biometric Consent Form in [Appendix VI](#)). If one parent objects in writing, then the school will not take or use a child's biometric data.

Parents/carers and students 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 students. For example, a pin number may be provided for students to access the cashless catering system if they wish.

Parents/carers and students can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student 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 student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric systems, for cashless catering and for door access, 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.

### **13. CCTV**

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [guidance](#) for the use of CCTV. 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.

Please see our CCTV policy for further details. Any enquiries about the CCTV system should be directed to Andrew Mathieson, Data Compliance Officer.

### **14. 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 students aged 18 and over, for photographs and videos to be taken of students 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 student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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

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

### **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 privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (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
- 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

## 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, pinned to notice/display boards, or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are required to change their passwords at regular intervals.
- Where personal information in a paper format needs to be taken off site, staff must take personal responsibility for keeping that data safe.
- Where personal data in an electronic format is taken off site it must be held on an encrypted laptop or encrypted pen drive.

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see Appendix II)
- 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 dispose of paper-based records by placing them in the Shred-it consoles, or in a confidential waste bag, both of which a third-party company then disposes of securely. Electronic files are overwritten or deleted. Where we use a third party to safely dispose of records on the school's behalf, we 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 I. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- An email containing personal data being sent to the incorrect recipient
- Dropping or leaving documents containing personal data in a public place
- Safeguarding information being made available to an unauthorised person
- Personal data being left unattended at a printer enabling unauthorised persons to read that information
- Opening a malicious email attachment or clicking on a link from an external or unfamiliar source, which leads to school's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data
- The theft of a school laptop containing non-encrypted personal data about students.

## **19. Breach notification data controller to data subject**

- For every breach the school will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk they will be notified as soon as possible and kept informed of actions and outcomes.



- The breach and process will be described in clear and plain language.
- If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Controller with support from the Data Protection Compliance Manager and DPO.
- Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.
- A post breach action plan will be put into place and reviewed.

## 20. 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.

## 21. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy was reviewed and updated when the Data Protection Bill received royal assent and became law in May 2018 (as the Data Protection Act 2018). From then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

## 22. Links with other policies

This data protection policy is linked to our:

- Freedom of Information Policy
- Freedom of Information publication scheme
- CCTV Policy
- Acceptable Use BYOD considerations (See [Appendix II](#))

## Appendix I: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO. The 'Data Breach Flowchart' outlines the process.

1. On finding or causing a breach, or potential breach, the staff member or data processor must **immediately** notify the Data Compliance Officer (DCO) in school who will then notify the Data Protection Officer (DPO).
2. The 'Data Breach form' will be completed and updated as the process progresses
3. 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
4. Evidence Collection
  - 4.1. It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO, it could also be used within criminal or civil proceedings.
  - 4.2. This process will be conducted by a suitable member of school staff, which may be the Data Management Compliance Officer or Data Protection Officer, but will be determined depending on the nature of the breach.
  - 4.3. Guidance may be required from external legal providers and police may be involved to determine the best way to secure evidence.
  - 4.4. A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored, possibly in a designated offsite facility.
5. The DPO will alert the DCO, the headteacher and the chair of governors
6. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary
7. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
8. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

- Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

9. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Breach and non-compliance log on the school's computer system (which may include one-drive for business)
10. Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. 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
11. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. 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.
12. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - 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
13. The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
14. 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)

15. Records of all breaches will be stored Breach and non-compliance log on the school's computer system (which may include one-drive for business)

**Actions to minimise the impact of data breaches**

The DPO, DCO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

## Appendix II: Acceptable Use / Bring Your Own Device Considerations

Guiseley School recognise that many staff choose to access school information from their own devices.

Any member of staff wishing to do this must be aware that they have a direct personal responsibility for ensuring that the device they choose to use has the benefit of encryption, that is above and beyond a simple password protection.

Staff must ensure that personal devices such as mobile smart phones, tablets and other portable electronic equipment are set to lock and only open with secured passcodes to prevent unauthorised access.

**If any member of staff uses a device without these safeguards in place it will be a disciplinary breach if data is unlawfully accessed by a third party.**

Encrypted pen drives are made available to all members of staff and are available from the Data Compliance Officer in school, Andrew Mathieson.

## Appendix III: Consent Form



# Parental Consent Form

Child's Name: ..... Form: .....

### 1. Photographs, Video and Media

<i>Note 1: In these instances it is only the photo image that would be published and not the name of your child</i>	Yes	No
May we use your child's photograph in printed publications that we produce for promotional purposes such as a prospectus or on project display boards? <sup>1</sup>		
May we use your child's image on our website? <sup>1</sup>		
May we record your child's image on video or webcam? <sup>1</sup>		
Are you happy for your child to appear in the media? <sup>1</sup> (for example in the local press, radio or TV)		
Are you happy for your child to appear on Social Media sites used by the school e.g. Twitter? <sup>1</sup>		
I give consent for my child to be included in any school or class Yearbook		
Do you consent for your child's name to be released for publication such that they may be identified as an individual or as part of a small group? For example raising money for charity that is recognised in the local media.		
I give consent for my child to be photographed for school group photos that may be bought by other families who have children in the photo.		
Do you consent for a professional photographer to take photographs and release to your family for sale? The photographer would have possession of the photos on their equipment, not school equipment.		

Can your child participate in events and performances that may be recorded or photographed and shared with the school community? <sup>1</sup>		
---	--	--

## 2. Careers & Workplace Placements

	Yes	No
I give consent for school to share details of my child with potential workplace placement providers		
I give consent to school to share details of my child with careers advisers		

## 3. School Work & Celebrating Successes

<i>Children may give their own consent for their work to be displayed as they hold the copyright</i>	Yes	No
I give consent for school to share details of my child's achievements within school by displays, certificates or other media that identifies them		
I give consent to school to share details of my child's achievements to celebrate their success at events within the school community		
I give consent for school to share details of my child's sporting activities for fixtures and achievements in school and in publications		

## 4. Internet Use

As part of the school's IT provision, we offer students access to the internet and email facilities. Our internet service provides a high level of protection and we audit student use. Students are required to agree to be bound by the school's terms of acceptable use.

	Yes	No
As the parent or carer, I give permission for my child to use electronic mail and the internet. I understand that students are held accountable for their own actions.		

## 5. Free School Meals and Pupil Premium

Please see the website below, which provides details of how the government may help parents with childcare costs. This applies to teenagers as well as younger children:

<https://www.childcarechoices.gov.uk/>

	Yes	No
I give consent for school to use my details, including National Insurance number, to check eligibility for Free School Meals and/or Pupil Premium		
I consent to the school to retain this information on file to continue to monitor eligibility		

## 6. School News Updates

<i>Please note: we cannot accept incoming text messages.</i>	Yes	No

I wish to be kept informed about school news and events, including PTA and ALPT news and events, and receive the newsletter and similar notifications		
I give consent to the school to use email on the email address I have provided.		
I consent to the school contacting me by email for the purpose of school information and reminders. I will ensure that I keep the school informed of my up to date email address at all times, or if the address is no longer in use.		
I give consent to the school to use text-messaging service on the mobile number I have provided.		
I consent to the school contacting me by text message for the purpose of school information and reminders. I will ensure that I keep the school informed of my up to date mobile number at all times, or if the number is no longer in my possession		

## 7. Third Parties at School

	Yes	No
I give consent to the school to share basic details with third party providers, such as music and sport providers, who may be engaged directly by me.		
I give consent to the school that they can share information about my child with organisations such as the Duke of Edinburgh scheme and World Challenge (Sixth Form).		

## 8. Medical

Guiseley School has a [Medical Policy](#), which is published on our website.

- If a student has a short-term medical condition that requires medication during school hours (e.g. antibiotics to cover a chest infection), a medication form is sent to the student's parent/carer to complete and confirm consent.
- We use an Individual Healthcare Plan for children with complex health needs, which includes consent to give medication and/or other treatments.
- We seek consent from the parent/carer before any referral to the School Health Nursing Service/Voluntary agencies/Aireborough Children's Services is made, unless the referral is a self-referral from a young person deemed competent.

We ask that you provide the following medical details for your child:

Doctors Practice	
Doctors Name	
Telephone Number	



Does your child suffer from any health problems? If 'YES' please complete an <b>Individual Healthcare Plan</b> .	Yes / No ( <i>Please circle/delete</i> )
Do you give consent for us to contact your child's Doctor?	Yes / No / Not applicable ( <i>Please circle/delete</i> )
Do you give consent for us to contact other professionals who are involved with your child?	Yes / No / Not applicable ( <i>Please circle/delete</i> )
Names and contact numbers of any professionals involved with your child, for example health visitors, speech therapists. If you provide these details we may contact them, letting you know of any approach we make.	
Please give details of any other problems/concerns of which the school should be aware to enable us to support your child.	
Please give details of any special requirements/medical conditions of parents/carers regarding access to the building or accessing information	

## 9. School Trips & Off Site Visits

Guiseley School seeks specific parental consent for students to participate in school trips and visits on a case by case basis.

Please note that when making arrangements for residential school trips it is necessary to share information about your child with the venue, accommodation and transport providers for legal and safeguarding reasons.

If travelling overseas this will also include immigration control.

Details about your child may be required by insurers.

For trips outside the UK, school staff and those supervising, travelling or arranging travel or accommodation may communicate with parents and carers using the contact information provided. At times, this may be using mobile communications, social media or other methods that may require data to be stored or travel outside of the approved EU locations. We believe that keeping parents and carers informed about the wellbeing of their children must be the priority. Data sharing in such cases will be limited to what is necessary.

<i>Note 1: In these instances it is only the photo image that would be published and not the name of your child</i>	Yes	No
I give consent for school to take photographs of my child whilst on school trips. <sup>1</sup>		

I give consent to school to take video and media footage of my child whilst on school trips <sup>1</sup>		
--	--	--

**10. Biometrics**

Please see the separate [Biometric consent form](#).

**Please note that when you provide consent, we will keep it on file over the course of your child's time at school. If anything changes, please let us know via email on [info@guiseleyschool.org.uk](mailto:info@guiseleyschool.org.uk) or in writing to the School Office.**

**Signed by Parent/Carer: ..... Date: .....**

## Appendix IV: Withdrawal of Consent Form (Pupil)



# Consent Withdrawal Form – on behalf of Pupil

**Please complete and deliver this form to the school office with your signature.**

Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where two parents share parental responsibility, or where PR is shared and the pupil is capable of expressing a view and there is conflict between the individuals the process of withdrawing consent will be subject to an evaluation and discussion to enable a decision to be reached that is considered to be in the pupil's best interests.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case, a senior member of school staff will discuss this with you.

### Withdrawal of consent on behalf of a pupil

I, \_\_\_\_\_ (Parent/Carer name in BLOCK CAPITALS), withdraw consent in respect of \_\_\_\_\_ (Pupil Name in BLOCK CAPITALS) for Guiseley School to process their personal data for the purpose of

\_\_\_\_\_  
\_\_\_\_\_, which was previously granted.

I confirm that I am \_\_\_\_\_ (Parent/Carer name in BLOCK CAPITALS) and that I have parental responsibility for the pupil.

Signed: \_\_\_\_\_ Date: \_\_\_\_\_

---

**Received in school by (Print name in BLOCK CAPITALS):**

Signature:

Dated:

## Appendix V: Withdrawal of Consent Form (Adult)



# Consent Withdrawal Form – Adult

**Please complete and deliver this form to the school office with your signature.**

Please note that as a school we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

### Withdrawal of consent for an Adult

I, \_\_\_\_\_ (name in BLOCK CAPITALS),

withdraw consent for Guisseley School to process my personal data for the purpose of

\_\_\_\_\_

\_\_\_\_\_, which was previously granted.

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

---

**Received in school by** (Print name in BLOCK CAPITALS):

Signature:

Dated:

**Actions:**

**Appendix VI: Biometric Consent**



**GUISELEY  
SCHOOL**

**Biometric Consent Form**

Child's name: ..... Form: .....

Child's name: ..... Form: .....

Child's name: ..... Form: .....

Child's name: ..... Form: .....

	Yes	No
I give consent to information from the finger scan of my child/children (named above) being taken and used as part of an automated biometric recognition system for access to cashless dining facilities, door access system and Sixth Form registration. I understand that I can withdraw this consent at any time in writing.		

Signed: .....

Name: .....

**Parent/Carer**

Date: .....

Signed: .....

Name: .....

**Parent/Carer**.....

Date: .....

*Please will you check with all parties who hold parental responsibility for your child that they give their consent.*

*Should you need School to send a consent form to somebody else with parental responsibility, please advise us in writing to our official address or by email to [info@guiseleyschool.org.uk](mailto:info@guiseleyschool.org.uk) . Thank you.*

## Appendix V11: Subject Access Request Form



# Subject Access Request Form

### Data Subject (person who information is about)

Title	
Name	
Date of Birth	
Year group (if child or young person)	

### Person making the request

Name	
Date of Birth	
Address	
Email Address	
Contact phone no	
Identification Evidence Provided (if required ) Passport Driving licence Or two forms of Utility bill within last 3 months Bank statement of last three months Council Tax bill Rent book	

### Status of person making request

Parent or person with Parental Responsibility	
---	--

Are you acting on their written authority (please provide a copy of the consent)	
If not the parent or with PR, what is your role?	

**Details of Data Requested**

I, ....., (*name in BLOCK CAPITALS*) hereby request that Guiseley School provide the data requested about me.

**Signature:** \_\_\_\_\_ **Dated:** \_\_\_\_\_

I, ....., (*name in BLOCK CAPITALS*) hereby request that Guiseley School provide the data requested about..... (*insert child's name in BLOCK CAPITALS*) on the basis of the authority that I have provided.

**Signature:** \_\_\_\_\_ **Dated:** \_\_\_\_\_

## Appendix VIII: Complaints form

### Personal Details:

Name:	
Address:	
Postcode:	
Daytime telephone number:	
Evening telephone number:	
E-mail:	

If applicable, name of child(ren) and form group/year at school:

Name	Form group/year

Your relationship to the school, e.g. parent, carer, neighbour, member of the public, student:

---



**What action, if any, have you already taken to try and resolve your complaint? Who did you speak to, when and what was the response?**

--

**What actions do you feel might resolve the problem at this stage?**

--

<b>Signature:</b>	
<b>Date:</b>	

---

**Official Use:**

Date of acknowledgment:	
By whom:	
Complaint referred to:	
Date:	