



GIGGLESWICK SCHOOL

DATA PROTECTION POLICY & PRIVACY NOTICE

Lead Author(s)	Bursar
Reviewed by	Senior Exec
Approval Committee	n.a.
Last review	January 2026
Review frequency	Biennial
Next Review	January 2028
Policy Type	Statutory

Contents

1. WHO WE ARE	5
2. WHAT THIS DATA PROTECTION POLICY AND PRIVACY NOTICE IS FOR	5
3. DEFINITIONS	6
4. APPLICATION OF THIS POLICY	6
5. RESPONSIBILITY FOR DATA PROTECTION	7
6. THE PRINCIPLES	7
7. LAWFUL GROUNDS FOR DATA PROCESSING	8
8. TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL	10
9. HOW THE SCHOOL COLLECTS DATA	10
10. WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH	11
10.1 Processing by third parties	11
10.2 Data sharing	11
11. KEEPING IN TOUCH AND SUPPORTING THE SCHOOL	11
12. ACCESS TO SENSITIVE DATA	12
12.1 Medical data	12
12.2 Safeguarding data	12
13. HOW LONG WE KEEP PERSONAL DATA	12
14. RESPONSIBILITIES OF SCHOOL STAFF FOR THE MANAGEMENT OF DATA	13
15. RIGHTS OF INDIVIDUALS	14
16. WHOSE RIGHTS.....	15

17. REQUESTS BY OR ON BEHALF OF PUPILS	16
17.1 Parental requests	16
18. REQUESTS THAT CANNOT BE FULFILLED	16
19. CONSENT	17
20. DIRECT MARKETING (PECR).....	18
21. INTERNATIONAL TRANSFERS OF PERSONAL DATA	18
22. CHILDREN’S CODE (AGE APPROPRIATE DESIGN CODE)	18
23. BIOMETRIC DATA IN SCHOOLS	18
24. RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30)	18
25. DATA SHARING CODE OF PRACTICE.....	19
26. LAW ENFORCEMENT PROCESSING (PART 3 DPA 2018)	19
27. POLICY GOVERNANCE AND DPIA TRIGGERS.....	19
28. DATA ACCURACY AND SECURITY	19
29. THIS POLICY	20
30. QUERIES AND COMPLAINTS THIS	20

1. WHO WE ARE

Giggleswick School is an independent school founded in 1512 whose principal place of business is at Giggleswick School, Settle, North Yorkshire BD24 0DE. We are a registered charity (registered number 1109826) and operate as a company limited by guarantee (number 5447105). Our activities comprise secondary and primary education in a boarding setting, along with short courses, fundraising, and letting of our facilities. Giggleswick School has two subsidiary companies, Giggleswick Services Ltd and Giggleswick International Ltd.

Giggleswick School comprises Giggleswick School, Giggleswick Preparatory School and Mill House Pre-School.

Under the Data Protection Act 2018 Giggleswick School identifies itself as a data controller.

2. WHAT THIS DATA PROTECTION POLICY AND PRIVACY NOTICE IS FOR

This **Privacy Notice** is intended to provide information about how Giggleswick School ("the School") will use (or "process") personal data about individuals including its staff, its current, past and prospective pupils, and their parents, carers or guardians (referred to in this policy as "parents"). Collectively, we refer to these individuals in the Privacy Notice as the School's community.

During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, their parents, its contractors and other third parties. The School, as data "controller", is liable for the actions of its staff and governors in how they handle this data.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the "UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The DPA 2018 includes specific provisions of relevance to independent schools: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

Data protection law has in recent years strengthened the rights of individuals and placed tougher compliance obligations on organisations including schools that handle personal information. The Information Commissioner's Office ("ICO") is responsible for enforcing data protection law in the UK, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

This Data Protection Policy and Privacy Notice seeks to lay out both the rights of individuals within the School community and the obligations placed on the School and its staff in relation to extant UK data protection legislation.

Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the School's obligations to its entire community. However, please note that the School also retains a separate Privacy Notice applicable to its staff and employees.

This **Privacy Notice** applies alongside any other information the School may provide about a particular use of personal data, for example when collecting data via an online or paper form.

This **Privacy Notice also** applies in addition to the School's other relevant terms and conditions and policies, including:

- any contract between the School and its staff or the parents of pupils;
- the School's policy on taking, storing and using images of children;

- the School's CCTV and biometrics policy;
- the School's retention of records policy;
- the School's safeguarding policy, pastoral policies, or health and safety policy, including as to how concerns or incidents are recorded; and
- the School's IT policies, including its Acceptable Use policy, eSafety policy, and Bring Your Own Device policy.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) will be subject to suitable training and/or policies commensurate with their role.

3. DEFINITIONS

Key data protection terms used in this data protection policy are:

- **[Data] Controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, the School (including by its governors) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a controller.
- **[Data] Processor** – an organisation that processes personal data on behalf of a controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Personal information (or 'personal data')**: any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.
- **Processing** – virtually anything done with personal data, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

4. APPLICATION OF THIS POLICY

This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

Those who handle personal data as employees or governors of the School are obliged to comply with this policy when doing so. For employees, breaches of this policy may result in disciplinary action. Accidental breaches of the law or this policy in handling personal data will happen from time to time, for example by human error, and will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as 'processors' on the School's behalf (in which case they will be subject to binding contractual terms) or as controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party controllers – which may range from other schools, to parents and appropriate authorities – each party will need a lawful basis to process that personal data, and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

If you are a volunteer or contractor, you will be a data controller in your own right, but the same legal regime and best practice standards set out in this policy will apply to you by law.

5. RESPONSIBILITY FOR DATA PROTECTION

The School has appointed the Bursar as Data Protection Coordinator who will deal with all requests and enquiries concerning the School's uses of your personal data (see section on 'Your Rights' below) and endeavour to ensure that all personal data is processed in compliance with this policy and the principles of applicable data protection legislation.

Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Coordinator at bursar@giggleswick.org.uk.

6. THE PRINCIPLES

The UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by controllers (and processors). These require that personal data must be:

1. Processed **lawfully, fairly** and in a **transparent** manner;
2. Collected for **specific and explicit purposes** and only for the purposes it was collected for;
3. **Relevant** and **limited** to what is necessary for the purposes it is processed;
4. **Accurate** and kept **up to date**;
5. **Kept for no longer than is necessary** for the purposes for which it is processed; and
6. Processed in a manner that ensures **appropriate security** of the personal data.

The UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;

- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments ("DPIA")); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

7. LAWFUL GROUNDS FOR DATA PROCESSING

Under the UK GDPR there are several different lawful grounds for processing personal data. One of these is consent. However, given the relatively high bar of what constitutes consent under the UK GDPR (and the fact that it can be withdrawn by the data subject) it is considered preferable for the School to rely on another lawful ground where possible.

One of these alternative grounds is 'legitimate interests', which is the most flexible basis for processing. However, it does require transparency and a balancing assessment between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notice, as the UK GDPR requires.

Other lawful grounds include:

- compliance with a legal obligation, including in connection with employment, engagement of services and diversity;
- contractual necessity, e.g. to perform a contract with staff or parents, or the engagement of contractors;
- a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

In order to carry out its ordinary duties to staff, pupils and parents, the School may process a wide range of personal data about individuals (including current, past and prospective staff, pupils or parents) as part of its daily operation.

Some of this activity the School will need to carry out in order to fulfil its legal rights, duties or obligations – including those under a contract with its staff, or parents of its pupils.

Other uses of personal data will be made in accordance with the school's legitimate interests', or the legitimate interests of another, provided that these are not outweighed by the impact on individuals and provided it does not involve special or sensitive types of data.

The School expects that the following uses may fall within that category of its (or its community's) "legitimate interests":

- For the purposes of pupil selection, to confirm the identity of prospective pupils and their parents, and retain a record if appropriate for the purposes of future applications or openings;
- To provide education services, including musical education, physical training or spiritual development, career services, and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs, including where such services are provided remotely (either temporarily or permanently);
- Maintaining relationships with alumni and the School community, including direct marketing or fundraising activity;

- For the purposes of donor due diligence, and to confirm the identity of prospective donors and their background and relevant interests;
- For the purposes of management planning and forecasting, research and statistical analysis, including that imposed or provided for by law (such as diversity or gender pay gap analysis and taxation records);
- To enable relevant authorities to monitor the School's performance and to intervene or assist with incidents as appropriate;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the School;
- To safeguard pupils' welfare and provide appropriate pastoral care;
- To monitor (as appropriate) use of the School's IT and communications systems in accordance with the School's IT Acceptable Use Policy;
- To make use of photographic images of pupils in school publications, on the School website and (where appropriate) on the School's social media channels in accordance with the School's policy on taking, storing and using images of children;
- For security purposes, including CCTV in accordance with the School's CCTV policy;
- For regulatory record keeping / compliance purposes in respect of immigration requirements, as an employer and/or visa sponsor;
- To carry out or cooperate with any school or external complaints, disciplinary or investigation process; and
- Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

In addition, the School may need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons may include:

- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example, for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of School trips who may need to be made aware of dietary or medical needs;
- To comply with public health requirements in respect of Covid-19 (or similar) testing, including managing on-site testing and/or processing the results of tests taken by pupils or other members of the School community, and sharing this information with the relevant health authorities;
- To provide educational services in the context of any special educational needs of a pupil;
- To provide spiritual education in the context of any religious beliefs;
- In connection with employment of its staff, for example DBS checks, welfare or pension plans;

- To run any of its systems that operate on biometric data, such as for security and other forms of pupil identification (for example, registering for meals);
- As part of any School or external complaints, disciplinary or investigation process that involves such data, for example if there are SEND, health or safeguarding elements; or
- For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with its legal obligations and duties of care.

8. TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

This will include by way of example:

- names, addresses, telephone numbers, e-mail addresses and other contact details;
- car details (for pupils who bring a car to School);
- biometric information;
- bank details and other financial information, e.g. about parents (or others) who pay fees to the School, and any other anti-money laundering information we are required to collect by law;
- past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- personnel files, including in connection with academics, employment or safeguarding;
- nationality and other immigration status information (such as right to study / work), including copies of passport information under the School's status as a Student Sponsor with the Home Office;
- where appropriate, information about individuals' health, and contact details for their next of kin;
- references given or received by the School about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils;
- correspondence with and concerning staff, pupils and parents (past and present); and
- images of pupils (and occasionally other individuals) engaging in school activities, and images captured by the School's CCTV system (in accordance with the School's policy on taking, storing and using images of children).

9. HOW THE SCHOOL COLLECTS DATA

Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual) or collected from publicly available resources.

10. WHO HAS ACCESS TO PERSONAL DATA AND WHO THE SCHOOL SHARES IT WITH

10.1 PROCESSING BY THIRD PARTIES

For the most part, personal data collected by the School will remain within the School, and will be processed by appropriate individuals in accordance with access protocols (i.e. on a 'need to know' basis). However, some functions are outsourced including cloud storage. In accordance with Data Protection Law, this type of external data processing is always subject to contractual assurances that personal data will be kept securely and used only in accordance with the School's specific directions.

10.2 DATA SHARING

Occasionally, the School will need to share personal information relating to its community with third parties, such as:

- professional advisers (e.g. lawyers, insurers and accountants);
- appropriate contractors, such as visiting coaches;
- the Giggleswick School Parents' Association (GSPA);
- examination boards;
- Stage 3 complaints panels, which may include independent panel members;
- Government/regulatory authorities (e.g. HMRC, DfE, NHS, police or the local authority).
- the alumni association, the Old Giggleswickians Committee (**with whom the School has a Data Sharing Agreement**).

All third-party data processors must have a written Data Processing Agreement (DPA) with the School, ensuring compliance with UK GDPR Article 28. Contracts must cover security measures, data retention, and breach response responsibilities.

11. KEEPING IN TOUCH AND SUPPORTING THE SCHOOL

The School will use the contact details of parents, alumni and other members of the School community to keep them updated about the activities of the School, or alumni and parent events of interest, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the School may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the School community, such as the Old Giggleswickians Committee, and the Giggleswick School Parents' Association (GSPA);
- Contact parents and/or alumni (including via the organisations above) by post and email in order to promote and raise funds for the School and provide information about school-related events, such as the schedule of activities for the Richard Whiteley Theatre;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the School's fundraising activities;
- Should you wish to limit or object to any such use, or would like further information about them, please contact bursar@giggleswick.org.uk in writing. You always have

the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School may need nonetheless to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

12. ACCESS TO SENSITIVE DATA

Particularly strict rules of access apply in the context of:

- medical records held and accessed only by the School medical staff; and
- pastoral or safeguarding files.

12.1 MEDICAL DATA

The School needs to process medical data to comply with statutory duties and to keep pupils and others safe, but the School will ensure only authorised staff can access information on a need-to-know basis. This may include wider dissemination if needed for school trips or for catering purposes. Express consent will be sought where appropriate.

However, a certain amount of any SEND pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

12.2 SAFEGUARDING DATA

Staff, pupils and parents are reminded that the School is under duties imposed by law and statutory guidance (including [Keeping Children Safe in Education](#) or KCSIE) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This may include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. The School uses a software application, CPOMS, to monitor child protection, safeguarding, SEND, attendance, behaviour, and other related matters. KCSIE also requires that, whenever a child leaves the School to join another school or college, his or her child protection file is promptly provided to the new organisation. The School will retain a copy in accordance with its retention policy for material related to safeguarding matters. For further information about this, please view the School's Safeguarding Policy.

13. HOW LONG WE KEEP PERSONAL DATA

The School will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason. Typically, the legal recommendation for how long to keep ordinary staff and pupil personnel files is up to seven years following departure from the School. However, incident reports and safeguarding files will need to be kept much longer, in accordance with specific legal requirements. If you have any specific queries about how this policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact bursar@giggleswick.org.uk. However, please bear in mind that the School may have lawful and necessary reasons to hold on to some data. Further information is available in the School's Data Retention Policy.

A limited and reasonable amount of data will be kept for archiving purposes. For example, where you have requested that we no longer keep in touch with you we will need to keep a record of the fact in order to fulfil your wishes.

14. RESPONSIBILITIES OF SCHOOL STAFF FOR THE MANAGEMENT OF DATA

14.1 RECORD-KEEPING

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to inform the School if they believe that any personal data is inaccurate or untrue or if you are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out below, whereby any individuals about whom they record information on School business (notably in emails and notes) digitally or in hard copy files may have the right to see that information. This absolutely must not discourage staff from making necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils and parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold these from such requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

14.2 DATA HANDLING

All staff have a responsibility to handle the personal data which they come into contact with fairly, lawfully, responsibly and securely and in accordance all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities such as safeguarding and IT security, so all staff should read and comply with the following policies:

- Safeguarding Policy
- IT Acceptable Use Policy.
- Data Retention Policy
- Taking, Storing and Using Images of Children Policy
- CCTV Policy

Responsible processing also extends to the creation and generation of new personal data / records, as above, which should always be done fairly, lawfully, responsibly and securely.

14.3 AVOIDING, MITIGATING AND REPORTING DATA BREACHES

One of the key obligations contained in the UK GDPR is on reporting personal data breaches. In accordance with Article 33 of the UK GDPR, controllers must report a personal data breach to the ICO within 72 hours where it is likely to result in a risk to individuals' rights and freedoms; if there is likely to be a high risk to individuals, the School must also inform affected individuals without undue delay. The School will assess all data breaches and if a breach poses a high risk to individuals' rights and freedoms the ICO and effected individuals will be notified in accordance with Article 33 of the UK GDPR.

In any event, the School must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If staff become aware of a personal data breach they must notify the Bursar and IT Manager. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision.

As stated above, the School may not need to treat the incident itself as a disciplinary matter – but a failure to report could result in significant exposure for the School, and for those

affected, and could be a serious disciplinary matter whether under this policy or the applicable staff member's contract.

14.4 CARE AND DATA SECURITY

More generally, we require all School staff (and expect all our contractors) to remain mindful of the data protection principles (see section 6 above), and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that effects daily processes: filing and sending correspondence, notably hard copy documents. Data handlers should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

We expect all those with management / leadership responsibilities to be particular champions of these principles and to oversee the swift reporting of any concerns about how personal information is used by the School to the Bursar, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

14.5 USE OF THIRD PARTY PLATFORMS / SUPPLIERS

As noted above, where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements (as required by the UK GDPR). It may also be necessary to complete a DPIA before proceeding – particularly if the platform or software involves any sort of novel or high risk form of processing (including any use of artificial intelligence ("AI") technology). Any request to engage a third party supplier should be referred to the IT Manager in the first instance, and at as early a stage as possible. Generally, the School receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments).

However, in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual) or collected from publicly available resources.

14.6 PROCESSING OF FINANCIAL / CREDIT CARD DATA

The School complies with the requirements of the PCI Data Security Standard ("PCI DSS"). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If you are unsure in this regard please seek further guidance from the Bursar. Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

14.7 STAFF GDPR TRAINING & RESPONSIBILITIES

All staff handling personal data must undergo annual GDPR training, with refresher sessions every six months for high-risk roles (e.g., IT, HR, admissions) as laid out in the Mandatory Staff Training Guidelines.

15. RIGHTS OF INDIVIDUALS

15.1 INDIVIDUAL RIGHTS

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor to refer to the correct legislation.

Individuals also have legal rights to:

- require the School to correct the personal data it holds about them if it is inaccurate;
- request the School erase their personal data (in certain circumstances);
- request that the School restrict its data processing activities (in certain circumstances);
- receive from the School the personal data it holds about them for the purpose of transmitting it in a commonly used format to another data controller; and
- object, on grounds relating to their particular situation, to any of the School's particular processing activities where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain rights are absolute and must be respected, specifically the right to:

- object to automated individual decision-making, including profiling (i.e. where a significant decision is made about the individual without human intervention);
- object to direct marketing; and
- withdraw one's consent where the School is relying on it for processing their personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

Any individual wishing to access or amend their personal data or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to bursar@giggleswick.org.uk.

If you consider that personal data we hold on you is inaccurate please let us know. However, the School will not necessarily delete or amend views, opinions, notes or records purely on the request of an individual who disputes the account, although we may keep a record of all parties' viewpoints.

15.2 SCHOOL RESPONSIBILITY IN RELATION TO INDIVIDUAL RIGHTS

In any event of a member of staff receiving or becoming aware of a request from an individual who is purporting to exercise one or more of their data protection rights, they are to inform the Bursar and/or IT Manager as possible.

The School will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits, which is generally one month, but actually fulfilling more complex or multiple requests may take 1-2 months longer. The School will be better able to respond quickly to smaller, targeted requests for information. If the request is manifestly excessive or similar to previous requests, the School may ask you to reconsider or charge a proportionate fee, but only where Data Protection Law allows it.

16. WHOSE RIGHTS

The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental authority to process personal data relating to pupils. Parents and pupils should be aware that this is not necessarily the same as the School relying on strict consent.

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the

pupil's consent, either alongside or in place of parental consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances. In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's IT: Acceptable Use Policy and the School Rules. Staff are under professional duties to do the same and this is covered in the Staff Code of Conduct.

17. REQUESTS BY OR ON BEHALF OF PUPILS

Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of the School, they have sufficient maturity to understand the request they are making (see section 'Whose Rights' below). Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the information in question is always considered to be the child's at law.

A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf. Moreover (if of sufficient age) their consent or authority may need to be sought by the parent making such a request. Pupils at Senior School aged e.g. 13 and above are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested, including any relevant circumstances at home. Slightly younger children and older Preparatory School children may however be sufficiently mature to have a say in this decision.

17.1 PARENTAL REQUESTS

It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The School may consider there are lawful grounds for sharing with or without reference to that pupil. Parents will in general receive educational and pastoral updates about their children. Where parents are separated, the School will in most cases aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child, court orders, or pastoral issues.

All information requests from, or on behalf of, pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case-by-case basis.

18. REQUESTS THAT CANNOT BE FULFILLED

You should be aware that certain data is exempt from the right of access. This may include information which identifies other individuals (and parents need to be aware that this includes their own children in certain limited situations), or information which is subject to legal privilege. The School is also not required to disclose any pupil examination scripts (or other

information consisting solely of pupil test answers, potentially including mock exam scripts or other types of exams / tests used to assess performance - although markers' comments may fall to be disclosed if they constitute pupil personal data). The School is also not required to provide examination or other test marks ahead of their ordinary publication date nor share any confidential reference given by the School for the purposes of the education, training or employment of any individual. These exemptions necessarily apply also in the context of teacher-assessed grades, where required in the absence of formal public examinations due to pandemic conditions.

You may have heard of the "right to be forgotten". However, we will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your (or your child's) personal data: for example, a legal requirement, or where it falls within a proportionate legitimate interest identified in this Privacy Notice. Generally, if the School still considers the processing of the personal data to be reasonably necessary, it is entitled to continue. All such requests will be considered on their own merits. The rights under Data Protection Law belong to the individual to whom the data relates. However, the School will often rely on parental authority to process personal data relating to pupils. Parents and pupils should be aware that this is not necessarily the same as the School relying on strict consent.

Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the pupil's consent, either alongside or in place of parental consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and all the circumstances. In general, the School will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the School's opinion, there is a good reason to do otherwise.

However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the School may be under an obligation to maintain confidentiality unless, in the School's opinion, there is a good reason to do otherwise; for example where the School believes disclosure will be in the best interests of the pupil or other pupils, or if required by law.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's IT: Acceptable Use Policy and the School Rules. Staff are under professional duties to do the same and this is covered in the Staff Code of Conduct.

19. CONSENT

Where the School is relying on consent as a means to process personal data, any person may withdraw this consent at any time (subject to similar age considerations as above). Please be aware however that the School may have another lawful reason to process the personal data in question even without your consent.

That reason will usually have been asserted under this Privacy Notice, or may otherwise exist under some form of contract or agreement with the individual (e.g. an employment or parent contract, or because a purchase of goods, services or membership of an organisation such as the alumni or parents' association has been requested).

20. DIRECT MARKETING (PECR)

The School's direct marketing activity (including fundraising communications to parents, alumni and supporters) must comply with the Privacy and Electronic Communications Regulations 2003 (PECR).

Electronic mail (e.g., email, SMS, in-app messages and direct social media messages) to individual subscribers generally requires prior consent or must meet the "soft opt-in" conditions. Where soft opt-in is relied upon, recipients must be given a clear, simple opportunity to opt out at the time of data collection and in every message. Business-to-business marketing may rely on legitimate interests, subject to PECR. Opt-out preferences (e.g., TPS/CTPS for calls) must be respected.

The lawful basis under UK GDPR for direct marketing will typically be consent or legitimate interests. PECR rules may require consent even where UK GDPR would permit legitimate interests. The School must keep records of consents and conduct a Legitimate Interests Assessment (LIA) where appropriate.

21. INTERNATIONAL TRANSFERS OF PERSONAL DATA

Any restricted transfers of personal data outside the UK must comply with UK GDPR Chapter V. Where no adequacy regulations apply, the School must use the ICO's standard data protection clauses – either the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU Standard Contractual Clauses – and complete a Transfer Risk Assessment (TRA). Where we engage overseas service providers (e.g., cloud or SaaS), the transfer mechanism and TRA must be documented in our Records of Processing.

22. CHILDREN'S CODE (AGE APPROPRIATE DESIGN CODE)

Where the School offers online services likely to be accessed by children under 18 (e.g., pupil portals, apps, learning platforms), we will apply the ICO's statutory Children's Code. This includes conducting DPIAs, setting high privacy by default, limiting profiling, geolocation and nudge techniques, ensuring age-appropriate transparency, and applying proportionate age assurance where needed.

23. BIOMETRIC DATA IN SCHOOLS

The School will only use automated biometric recognition systems (e.g., fingerprints or facial recognition) in compliance with the Protection of Freedoms Act 2012 and data protection law. We will: (a) notify each parent of the intention to use a child's biometric data; (b) obtain consent from at least one parent; (c) not process where the child or any parent objects; and (d) provide reasonable alternatives. Biometric data is "special category" personal data and requires an appropriate lawful basis and safeguards (including an Appropriate Policy Document where Schedule 1 conditions apply).

24. RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30)

The School maintains a record of processing activities (RoPA) covering: purposes; categories of data subjects and personal data; recipients; international transfers and safeguards;

retention schedules; and a general description of technical and organisational security measures. Processors engaged by the School must maintain their own Article 30 records.

25. DATA SHARING CODE OF PRACTICE

The School follows the ICO's Data Sharing Code of Practice when sharing data with third-party controllers. Before sharing, we will consider necessity and proportionality, identify the lawful basis (and any special category conditions), conduct due diligence on recipients, and (where appropriate) put in place a Data Sharing Agreement setting out roles, security, retention, and individuals' rights.

26. LAW ENFORCEMENT PROCESSING (PART 3 DPA 2018)

Sharing personal data with competent authorities (e.g., police) for law enforcement purposes may be subject to Part 3 of the Data Protection Act 2018. Where applicable, we will follow the specific regime for law enforcement processing, ensuring appropriate logging, safeguards, and respect for applicable rights and exemptions. For non-law-enforcement purposes, UK GDPR/Part 2 of the DPA 2018 applies.

27. POLICY GOVERNANCE AND DPIA TRIGGERS

The School will complete Data Protection Impact Assessments for processing that is likely to result in high risk, including: use of children's data in online services; large-scale use of special category or biometric data; systematic monitoring; novel technologies (including AI); and international transfers lacking adequacy. This policy will be reviewed annually and whenever material legislative or regulatory updates occur.

28. DATA ACCURACY AND SECURITY

The School will endeavour to ensure that all personal data held in relation to an individual is as up to date and accurate as possible. Individuals must please notify bursar@giggleswick.org.uk of any significant changes to important information, such as contact details, held about them.

An individual has the right to request that any out-of-date, irrelevant or inaccurate or information about them is erased or corrected (subject to certain exemptions and limitations under Data Protection Law): please see above for details of why the School may need to process your data, of who you may contact if you disagree.

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals, including policies around use of technology and devices, and access to school systems. All staff and governors will be made aware of this policy and their duties under Data Protection Law and receive relevant training.

29. THIS POLICY

The School will update this Privacy Notice from time to time. Any substantial changes that affect your rights will be provided to you directly as far as is reasonably practicable.

30. QUERIES AND COMPLAINTS THIS

Any comments or queries on this policy should be directed to the Bursar at bursar@giggleswick.org.uk

If an individual believes that the School has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise the school complaints procedure and should also notify the Bursar. The School can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with the School before involving the regulator.