



# Policy

## Data Protection Policy and Privacy Notice

### Data Protection Policy

#### Introduction

Data protection is an important legal compliance issue for Oakham School. 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 (in a manner more fully detailed in the School's Privacy Notice). The School, as "data controller", is liable for the actions of its staff and trustees in how they handle data. It is therefore an area where all staff have a part to play in ensuring we comply with and are mindful of our legal obligations, whether that personal data handling is sensitive or routine.

UK data protection law consists primarily of the UK version of the General Data Protection Regulation (the 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, and will typically look into individuals' complaints routinely and without cost, and has various powers to take action for breaches of the law.

The Trustees of Oakham School acknowledge their overall responsibility for ensuring that:

- Personal information relating to current and former pupils, parents and staff is processed in accordance with Education Regulations and all other statutory provisions, including the requirements of the GDPR and DPA 2018 and subsequent legislation;
- All members of staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities. Any enquiry relating to Data Protection should be addressed in writing to the Chief Operating Officer, who is Oakham School's Data Protection Controller (DPC).

This data protection policy and privacy notice applies to Oakham School, the Old Oakhamian (OO) Club and the Oakham Foundation, collectively referred to as Oakham School within this document.

## 1. 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 is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

- **Data processor** – an organisation that processes personal data on behalf of a data 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 information, 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.

## 2. 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 trustees 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 “data processors” on the School’s behalf (in which case they will be subject to binding contractual terms) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers – which may range from other schools, to parents, to appropriate authorities, to casual workers and volunteers – 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.

## 3. Person responsible for Data Protection at the School

The School has appointed the Chief Operating Officer (“COO”), William Hawkes, as the Data Protection Controller who will 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 Controller

## 4. The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data 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 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); 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.

## 5. Lawful grounds for data processing

Under the 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 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 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.

## 6. Headline responsibilities of all staff

### 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 recording necessary and sometimes difficult records of incidents or conversations involving colleagues or pupils, 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.**

### **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 with the staff handbook and 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

- ICT and mobile phone acceptable use policy
- Pupil record keeping policy
- Parent and guardians communication policy
- Social media policy
- Staff digital acceptable use policy
- Child protection 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.

### **Avoiding, mitigating and reporting data breaches**

One of the key obligations contained in the GDPR is on reporting personal data breaches. Data controllers must report certain types of personal data breach (those which risk an impact to individuals) to the ICO within 72 hours.

In addition, data controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms. 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 COO. 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.

### **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 3 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 they 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 COO, and to identify the need for (and implement) regular staff training. Staff must attend any training we require them to.

## **7. Rights of Individuals**

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 data 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. If you become aware of a subject access request (or indeed any communication from an individual about their personal data), you must tell the COO as soon as possible.

Individuals also have legal rights to:

- require us to correct the personal data we hold about them if it is inaccurate;
- request that we erase their personal data (in certain circumstances);
- request that we restrict our data processing activities (in certain circumstances);
- receive from us the personal data we hold 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 our 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 we are 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).

In any event, however, if you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the COO as soon as possible.

## **8. Data Security: online and digital**

The School must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

- no member of staff is permitted to remove personal data from School premises, whether in paper or electronic form and wherever stored, without prior consent of the Head or the COO.
- No member of staff should provide personal data of pupils or parents to third parties, including a volunteer or contractor, unless there is a lawful reason to do so.
- Where a worker is permitted to take data offsite on memory sticks or personal devices it will need to be encrypted.
- Use of personal email accounts or unencrypted personal devices by trustees or staff for official School business is not permitted.

## **9. 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 Finance 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.

## **10. Failure to Comply With This Policy**

Oakham School will treat any failure to comply with this Policy very seriously and shall regard it as a matter for internal discipline in accordance with the terms of the Disciplinary Procedures.

*It is in everyone's interests to get data protection right and to think carefully about data protection issues: this means handling all personal information with which you come into contact fairly, lawfully, securely and responsibly.*

*A good rule of thumb here is to ask yourself questions such as:*

- Would I be happy if my own personal information were being used (for example, shared with a third party) in the way I am proposing? Would I expect it?*
- Would I wish to stand by how I have recorded this information in an email or official record if the person concerned was able to see it?*
- What would be the consequences of my losing or misdirecting this personal data?*

*Data protection law is therefore best seen not as oppressive red tape, or a reason not to do something necessary or important, but a code of useful and sensible checks and balances to improve how handle and record personal information and manage our relationships with people. This is an important part of the School's culture and all its staff and representatives need to be mindful of it.*

**William Hawkes**  
**Chief Operating Officer**  
**8 May 2021**

## Privacy Notice

### COVID-19 RELATED PROCESSING

**While pandemic conditions persist, the School may need to collect, share and otherwise process personal data in accordance with Government guidance. This may be for reasons not specifically set out in this Privacy Notice but always for the purposes of protecting public and individual health by seeking to limit the spread of coronavirus (COVID-19).**

### What this privacy notice is for

This **Privacy Notice** is intended to provide information about how 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.

This information is provided because Data Protection Law gives individuals rights to understand how their data is used. Staff, parents and pupils are all encouraged to read this Privacy Notice and understand the school's obligations to its entire community.

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;
- any policies or notices applicable to staff concerning the handling of personal data;
- the school's policy on taking, storing and using images of children;
- the school's CCTV and/or biometrics policy;
- the school's retention of records policy;
- the school's safeguarding, pastoral, or health and safety policies, including as to how concerns or incidents are recorded; and
- the school's IT policies, including its Acceptable Use policy, Social Media policy, eSafety policy, WiFi policy, Remote Working 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.

### Responsibility for data protection

- The School has appointed the Chief Operating Officer ("COO) as the Data Protection Controller who will deal with all your 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 Data Protection Law.

The COO can be contacted by emailing [rpr@oakham.rutland.sch.uk](mailto:rpr@oakham.rutland.sch.uk)

### Why the School needs to process personal data

In order to carry out its ordinary duties to staff, pupils and parents, the school needs to 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 will 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 tax, diversity or gender pay gap analysis);
- 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 and current 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' health and 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 will on occasion 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 will 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 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 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, union membership or pension plans;
- 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, health and safety and immigration / visa sponsorship compliance) and to comply with its legal obligations and duties of care.

### **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 (about those who use our car parking facilities);
- bank details and other financial information, e.g. about parents (or others) who pay fees to the school, and any 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 (e.g. right to work / study), including copies of passport information or full passport copies;
- where appropriate, information about individuals' health and welfare, and contact details for their next of kin;
- references given or received by the school about pupils, and relevant 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);

### **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 will be supplied by third parties (for example another school, or other professionals or authorities working with that individual); or collected from publicly available resources .

### **Who has access to personal data and who the school shares it with**

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 only in accordance with access protocols (i.e. on a 'need to know' basis). However, some functions are outsourced including [e.g. HR, accounting, IT, cloud storage / records management, monitoring, mailing]. 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.

Data sharing. Occasionally, the school – including its [trustees / governing board] – will need to share personal information relating to its community of staff, pupils and parents with third parties, such as:

- the School's parent teacher committee, Old Oakhamian organisation, etc.
- appropriate contractors, such as visiting music teachers;
- professional advisers (e.g. lawyers, insurers, PR advisers and accountants);
- examination boards;
- Stage 3 complaints panels, which will include independent panel members;
- third parties and their advisers in the event of a possible or actual sale, merger or other restructuring of the school; and
- government authorities (e.g. HMRC, DfE, CAF/CASS, police, Home Office, a relevant public health / NHS body and / or local authority) and/or appropriate regulatory bodies e.g. the **Teaching Regulation Agency**, the **Independent Schools Inspectorate**, the **Charity Commission**, etc..
- Occasionally the school trustee] will need to process parent or pupil information, such as when a complaint is raised (and in accordance with the School Complaints Procedure, this may also require the involvement of independent panel members).

### **Access to sensitive data**

Particularly strict rules of access apply in the context of "special category" data, most notably:

- medical records; and
- pastoral or safeguarding files.

Medical data. The school needs to process such information 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.

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 is likely to include file notes on personnel or safeguarding files, low-level concerns records kept about adults, and in some cases referrals to relevant authorities such as the LADO or police.

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.

### **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 7 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 our retention policy is applied, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact the Chief Operating Officer. However, please bear in mind that the school will often have lawful and necessary reasons to hold on to some personal data **even following such request**.

A limited and reasonable amount of information will be kept for archiving purposes, for example; and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

Details are available in the school's records retention policy.

### **Keeping in touch and supporting the school**

The School and/or any relevant other organisation, e.g. alumni / development, 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 will 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 OO society, parent teacher committee, etc.
- 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, where appropriate, other worthy causes;
- Collect information from publicly available sources about parents' and former pupils' occupation and activities, in order to maximise the School's fundraising potential.
- Should you wish to limit or object to any such use, or would like further information about them, please contact the Chief Operating Officer in writing. You always have the right to withdraw consent, where given, or otherwise object to direct marketing or fundraising. However, the School is nonetheless likely to retain some of your details (not least to ensure that no more communications are sent to that particular address, email or telephone number).

### **Your rights**

Individuals (both pupils and parents) have various rights under Data Protection Law to access and understand their own personal data held and processed by the school, and in some cases ask for it to be erased or amended, or to have it transferred elsewhere, or for the school to stop processing it – but subject to certain exemptions and limitations.

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, e.g. those involving third party information, may take 1-2 months longer).

- Rights of access, etc.

The School will be better able to respond quickly to smaller, targeted requests for information made during term time. If the request for information is manifestly excessive or similar to previous requests, the school may ask you to reconsider, or require a reasonable fee for the administrative costs of complying with the request, or in certain cases refuse the request (but only where Data Protection Law allows it, and in accordance with relevant regulatory guidance).

If you consider that the 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.

- Requests that cannot be fulfilled

You should be aware that GDPR rights (including the right of access) are limited to your own personal data, and certain data is exempt. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by the school, or documents prepared in connection with a legal action, or where a duty of confidence is owed by a legal adviser).

The School is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers, potentially including in mock exam scripts or other types of exams / tests used to assess performance – although markers' comments may still be disclosable 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 held by the School that was (or will be) given for the purposes of the education, training, appointment 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. Please see our separate exam information notice which explains what information will be provided to all relevant pupils, and when, in respect of their grades.

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.

- 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). A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's. For older pupils, the parent making the request may need to evidence their child's authority for the specific request. Requests not considered in the child's best interests may sometimes be refused.

Pupils 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 may however be sufficiently mature to have a say in this decision, depending on the child and the circumstances.

- Parental requests, etc.

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, in accordance with the Parent Contract. 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, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

- 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). Examples where we do rely on consent are: e.g. certain types of uses of images, certain types of fundraising activity. Please be aware however that the school may not be relying on consent but 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 an alumni or parents' association has been requested).

- 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 or notice for the necessary ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that this is not necessarily the same as the school relying on strict consent (see section on Consent above).

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.

### **Pupil consent**

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. That is 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 relevant policies and the school rules. Staff are under professional duties to do the same covered under the relevant staff policy.

### **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 the COO 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.

### **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.**

### **Queries and complaints**

Any comments or queries on this policy should be directed to the COO using the following contact details : [rpr@oakham.rutland.sch.uk](mailto:rpr@oakham.rutland.sch.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 / grievance] procedure and should also notify the COO. You 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.

**William Hawkes  
Chief Operating Officer  
8 May 2021**

**APPENDIX ONE**

**Data Protection Policy Oakham School – Data Subject Access Form**

Enquirer's Surname .....

Enquirer's Forenames .....

Enquirer's Address .....

..... Enquirer's Postcode .....

Email Address ..... Home Phone Number .....

Mobile No .....

Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?  
YES / NO

If NO, please contact the Chief Operating Officer to determine whether or not we need to have express written permission from the 'Data Subject' to divulge the requested information to you. N.B. this is generally necessary for all information, other than Educational Progress Reports requested by parents.

Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about? YES / NO

If NO, please state the nature of your relationship with the data subject. Please note that the School may require proof of identity before disclosing any data.

.....

Name and Date of Birth of child or children about whose personal data records you are enquiring

Name ..... D.O.B .....

Name ..... D.O.B .....

Description of information or topic(s) requested

.....

.....

.....

Please despatch reply to: (if different from enquirer's details as stated on this form) Name

.....

Address .....

..... Postcode .....

If applicable, I undertake to pay Oakham School an administration fee prior to the requested information being sent to me in accordance with any agreement with the Chief Operating Officer.

Signature of data subject or subject's parent/guardian

.....

Printed name of person signing: .....

Date: .....

**APPENDIX TWO**

**Data Protection Policy Oakham School – Data Subject Consent To Access Form**

Data Subject's Surname ..... Data Subject's Forenames .....

Data Subject's Address .....

.....

Data Subject's Postcode ..... Email Address .....

Home Phone Number ..... Mobile No .....

Enquirer's Surname .....

Enquirer's Forenames .....

Enquirer's Address .....

.....

Enquirer's Postcode..... Email Address .....

Home Phone Number ..... Mobile No .....

Description of information or topic(s) requested

.....

.....

.....

Please despatch reply to: (if different from enquirer's details as stated on this form)

Name .....

Address .....

.....

Postcode .....

I understand that I am able in law to withhold this information from the Enquirer(s) and despite my right to withhold this data; I hereby consent to the School releasing the Subject Data to the Enquirer(s).

Signature of data subject .....

Printed name of person signing .....

Date signed .....