



ORWELL PARK SCHOOL
Nacton, Ipswich, IP10 0ER

DATA PROTECTION POLICY AND PROCEDURE

Date:	April 2025
Status:	Final
Review Date:	April 2027

SOL 04/2025

ORWELL PARK SCHOOL DATA PROTECTION POLICY AND PROCEDURES

INTRODUCTION

This policy outlines how Orwell Park School collects, processes, and protects personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It applies to all individuals including current, past, and prospective pupils, and their parents, carers or guardians (collectively referred to as "parents"), as well as staff, volunteers, governors, and service providers. This policy supplements the School's terms and conditions and other relevant notices (e.g. on the use of images). It also sets out the measures in place to protect personal data.

Anyone who works for, or acts on behalf of, the School (including staff, volunteers, governors and service providers) should also be aware of and comply with the School's data protection policy; for staff it also provides further information about how personal data about those individuals will be used.

POLICY STATEMENT

Orwell Park School recognises its responsibilities to protect data and takes this responsibility seriously. The Governors of the school delegate responsibility for arrangements for data protection to the Headmaster, who empowers the Bursar with responsibility for day to day operations to protect data. Overview of this important area will be provided by the governors safeguarding committee.

RESPONSIBILITY FOR DATA PROTECTION

The Governors delegate oversight of data protection to the Headmaster, who in turn delegates operational responsibility to the Bursar. The Data Protection Officer (DPO) is the Bursar, who reports to senior management and acts with independence to ensure compliance with data protection laws.

The School's registration with the Information Commissioner's Office (ICO) is under reference Z5741401.

ARRANGEMENTS FOR DATA PROTECTION

The School will do its utmost to protect data by designing a system of controls and operating in such a way as to comply with the DPA and UK GDPR and fulfil the aims and the "spirit" of these items of legislation; the data protection principles and in respect of the rights of an individual. Working with the DPO a team will be established to fulfil these responsibilities; the School data protection team (the team) will be established for routine arrangements in support of these aims. The team will monitor school arrangements and provide assistance to staff in management of data. Any new work or business systems that are introduced to the school will be subject to a risk assessment (or privacy impact assessment) to identify any possible hazards to the school system for data protection; additional measures including controls can therefore be identified to reduce any risk levels to an acceptable level. The School will operate its data protection arrangements in accordance with the 6 data protection principles (under the UK GDPR), as follows:

1. Lawfulness, fairness and transparency – data processing must meet the requirements of the UK GDPR; what is processed must match with how it has been described and the subject must be aware of what data processing must be completed.
2. Purpose Limitations – Personal data can only be obtained for specified, explicit and legitimate purposes.

3. Data minimisation – Data collected on a subject should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy – Data must be accurate and where necessary kept up to date.
5. Storage Limitations – Personal data should be kept in a form which permits identification of data subjects for no longer than necessary.
6. Integrity and Confidentiality – requires processors to handle data in a manner ensuring appropriate security of the personal data including protection.

The School recognises the rights of an individual stated under UK GDPR which are as follows:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

OPS PRIVACY NOTES

Individual Privacy notes for staff, pupils, parents and carers, and alumni and supporters is set out in ANNEX's C through to F.

TYPES OF PERSONAL DATA PROCESSED BY THE SCHOOL

The School may process a wide range of personal data about individuals including current, past and prospective pupils and their parents as part of its operation, including 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 regularly);
- Bank details and other financial information, e.g. about parents who pay fees to the school;
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
- 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; 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);

Generally, the School receives personal data from the individual directly (or, in the case of pupils, from parents). 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. The School may, from time to time, need to process "sensitive personal data" regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be

processed by the School with the explicit consent of the appropriate individual, or as otherwise permitted by the Act.

The School does not use data for any automatic decision making and does not undertake any automatic data processing.

USE OF PERSONAL DATA BY THE SCHOOL

The School will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents;
- To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the school community;
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the School's performance;
- 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 (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;
- To monitor 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 on the school's social media channels in accordance with the school's policy on taking, storing and using images of children;
- To undertake some targeted marketing activities the School may share personal data with advertisers such as Facebook/Instagram/Meta and Google for the purpose of promoting events and activities at Orwell Park via these advertising platforms;
- For security purposes, and for regulatory and legal purposes (for example child protection and health and safety) and to comply with its legal obligations; and

Where otherwise reasonably necessary for the School's purposes, including to obtain appropriate professional advice and insurance for the School.

The School will use a privacy note to inform parents, staff and interested parties about arrangements for data protection and their rights within these arrangements and under Data protection Law.

RETENTION OF DATA

The School will be required to retain certain data and will follow best practice in doing so; an outline of the data retention periods to be used by the school is attached at Annex A to this policy.

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, including by sending updates and newsletters, by email and by post. Where appropriate the School may seek consent for holding and using this information from individuals concerned. 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 Foundation, Friends of Orwell or Old Orwellians 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;

Should you wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing.

RIGHTS OF ACCESS TO PERSONAL DATA ("SUBJECT ACCESS REQUEST")

Individuals have the right under the Act and UK GDPR to access to personal data about them held by the School, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the Headmaster.

The School will endeavour to respond to any such written requests (known as "subject access requests") as soon as is reasonably practicable and in any event within statutory time-limits which is 30 days.

Certain data is exempt from the right of access under the Act and UK GDPR. This may include information which identifies other individuals, or information which is subject to legal professional privilege. The School is also not required to disclose any pupil examination scripts (though examiners' comments may not be disclosed), nor any reference given by the School for the purposes of the education, training or employment of any individual.

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. Pupils aged 12 or over are generally assumed to have this level of maturity, although this will depend on both the child and the personal data requested. All subject access requests from pupils will therefore be considered on a case by case basis. A person with parental responsibility will generally be expected to make a subject access request on behalf of pupils. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf.

WHOSE RIGHTS

The rights under the Act belong to the individual to whom the data relates. However, the School will in most cases rely on parental consent to process personal data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is

more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.

In general, the School will assume that pupils consent to 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 will 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.

Pupils are required to respect the personal data and privacy of others, and to comply with the School's IT acceptable use and behaviour policies and the School rules.

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 should notify the School Office or failing this the DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act and UK GDPR) and may do so by contacting the DPO in writing.

INTERNATIONAL DATA TRANSFERS

Where personal data is transferred outside the UK (e.g. via cloud services), appropriate safeguards will be in place to ensure lawful and secure processing.

DATA SECURITY

Technical and organisational measures are in place to ensure data security. Staff receive regular training, and data access is restricted to authorised individuals.

DATA BREACH

The School will take appropriate technical and organisational steps to ensure the security of personal data about individuals. All staff will be made aware of this policy and its supporting procedures as well as their duties under the Act. The School will endeavour to protect data by designing a system and operating in such a way to fulfil these aims. In the event of a loss of adequate protection levels around personal data such that personal data is inadvertently disclosed, stolen or destroyed the School will react as soon as possible to minimise the potential impact of any such loss or data breach. Any possible data breaches must be reported to the DPO as quickly as possible; the DPO will assess the situation and then make a decision on whether the breach should be reported to the ICO using the following guidance on reporting from the office of the ICO:

“Where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social advantage.”

If necessary the DPO will notify the ICO and ensure the data breach is added to the Data Breach Log. Steps to recover the data will then be taken and the relevant individuals informed of the data breach. When all steps have been completed the incident will be reviewed to identify any actions to mitigate possible future data losses. Information on the School data breach procedures is contained in Annex B.

QUERIES AND COMPLAINTS

Any comments or queries on this policy should be directed to the DPO using the following contact details:

Email: DPO@orwellpark.org or via the school website

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Act, they should utilise the school complaints procedure and should also notify the DPO.

Link with other procedures

This policy links with the following school policies:

- Complaints policy
- Whistleblowing policy
- Discipline policy (if any allegations of misconduct are proven)
- OPS IT policies and user instructions

ORWELL PARK SCHOOL TABLE OF DATA RETENTION PERIODS: SOURCE ISBA

Type of Record/Document	<u>Suggested</u> ¹ Retention Period
<u>EMAILS ON SERVER</u> - Pupil email account - Staff emails (incl. Governors)	Delete upon leaving school, or within one year. Routine deletion of historic email after 2-3 years, and delete account within 1 year of leaving school. Unless deemed necessary for emails to be kept for specific purposes (eg. financial correspondence with debtors).
<u>SCHOOL-SPECIFIC RECORDS</u> - Registration documents of School - Attendance Register - Minutes of Governors' meetings - Annual curriculum - Pupil work (exercise books)	Permanent (or until closure of the school) 6 years from last date of entry, then archive as above. 6 years from date of meeting From end of year: 3 years From year end 1 year for class records: eg marks /exercise books/ timetables / assignments)
<u>INDIVIDUAL PUPIL RECORDS</u> - Admissions: application forms, assessments, records of decisions - Student Immigration Records - Examination results (external or internal) - Pupil file including: - Pupil reports - Pupil performance records - Pupil medical records - Special educational needs records (<i>to be risk assessed individually</i>)	NB – this will generally be personal data 25 years from date of birth (or, if pupil not admitted, up to 7 years from that decision). If unsuccessful: up to 1 year. Duration of student sponsorship plus min. 1 year. 7 years from pupil leaving school ALL: 25 years from date of birth (subject to where relevant to safeguarding considerations: any material which may be relevant to potential claims should be kept for the lifetime of the pupil). Date of birth plus up to 35 years (allowing for special extensions to statutory limitation period)
<u>SAFEGUARDING</u> ¹ - Policies and procedures - DBS disclosure certificates (if held) - Accident / Incident reporting	NB – please read notice at the top of this note Keep a permanent record of historic policies <u>No longer than 6 months</u> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself. Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.

Child Protection files	If a referral has been made / social care have been involved or child has been subject of a multi-agency plan – indefinitely. If low level concerns, with no multi-agency act – apply applicable school low-level concerns policy rationale (this may be 25 years from date of birth OR indefinitely).
<u>CORPORATE RECORDS (where applicable)</u> - Certificates of Incorporation - Minutes, Notes and Resolutions of Boards or Management Meetings - Shareholder resolutions - Register of Members/Shareholders - Annual reports	<u>eg where schools have trading arms</u> Permanent (or until dissolution of the company) Minimum – 10 years Minimum – 10 years Permanent (minimum 10 years for ex-members/shareholders) Minimum – 6 years
<u>ACCOUNTING RECORDS</u> - Accounting records (<i>normally taken to mean records which enable a company's accurate financial position to be ascertained & which give a true and fair view of the company's financial state</i>) - Tax returns - VAT returns - Budget and internal financial reports	Minimum – 6 years for private UK companies (except where still necessary for tax returns) Minimum – 6 years for UK charities (and public companies) from the end of the financial year in which the transaction took place Internationally: can be up to 20 years depending on local legal/accountancy requirements Minimum – 6 years Minimum – 6 years Minimum – 6 years
<u>CONTRACTS AND AGREEMENTS</u> - Signed or final/concluded agreements (<i>plus any signed or final/concluded variations or amendments</i>) - Deeds (or contracts under seal)	Minimum – 7 years from completion of contractual obligations or term of agreement, whichever is the later Minimum – 13 years from completion of contractual obligation or term of agreement
<u>INTELLECTUAL PROPERTY RECORDS</u> - Formal documents of title (trade mark or registered design certificates; patent or utility model certificates) - Assignments of intellectual property to or from the school - IP / IT agreements (including software licences and ancillary agreements eg maintenance; storage; development; coexistence agreements; consents)	Permanent (in the case of any right which can be permanently extended, eg trade marks); otherwise expiry of right plus minimum of 7 years. As above in relation to contracts (7 years) or, where applicable, deeds (13 years). Minimum – 7 years from completion of contractual obligation concerned or term of agreement
<u>EMPLOYEE / PERSONNEL RECORDS</u> - Single Central Record of employees - Personnel files including recruitment checks including Contracts of employment	<u>NB this will contain personal data</u> Keep a permanent record that mandatory checks have been undertaken. 7 years from end of contract of employment; <u>do not delete any information which may be relevant to historic safeguarding claims.</u>

- Employee appraisals or reviews - Payroll, salary, maternity pay records - Pension or other benefit schedule records - Job application and interview/rejection records (unsuccessful applicants) - Immigration records - Tier 2 migrant worker sponsor records	Duration of employment plus minimum of 7 years Minimum – 6 years Possibly permanent, depending on nature of scheme Minimum 3 months but no more than 1 year Minimum – 2 years from end of employment Minimum – 1 year from end of employment
Health records relating to employees	7 years from end of contract of employment
Records of low-level concerns about adults	At least until end of employment, then subject to review for relevance. (eg. 7 years from end of employment is they have ongoing relevance for employment claims, longer if necessary for safeguarding purposes/claims.
<u>INSURANCE RECORDS</u>	
- Insurance policies (will vary – private, public, professional indemnity) - Correspondence related to claims/renewals/ notification re: insurance	Duration of policy (or as required by policy) plus a period for any run-off arrangement and coverage of insured risks: ideally, until it is possible to calculate that no living person could make a claim. Minimum – 7 years
<u>ENVIRONMENTAL, HEALTH & DATA</u>	
- Maintenance logs - Accidents to children - Accident at work records (staff) - Staff use of hazardous substances - Risk assessments (carried out in respect of above) - Data protection records documenting processing activity, data breaches	10 years from date of last entry 25 years from birth (longer for safeguarding) Minimum – 4 years from date of accident, but review case-by-case where possible Minimum – 7 years from end of date of use 7 years from completion of relevant project, incident, event or activity. No limit: as long as up-to-date and relevant (as long as no personal data held)

Footnotes:

1. The High Court has found that a retention period of 35 years was within the bracket of legitimate approaches for retaining safeguarding records. IICSA has recommended that, for child sexual abuse records, the period should be 75 years, and subject to regular review. The ICO (Information Commissioner's Office) also expects to see a regular review policy in place (e.g. every 6 years), although the High Court also held that could be a disproportionate use of resource for many organisations' safeguarding teams. The position is likely to be different for records of low-level concerns about adults, which should only be kept in line with employment records unless likely to be relevant for historic abuse claims or a specific safeguarding need.

ORWELL PARK SCHOOL DATA BREACH PROCEDURES

1. Introduction. A data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
2. Data breaches are to be reported to the DPO where they are likely to result in a risk to the rights and freedoms of individuals, this will need to be assessed on a case by case basis and entered into the Data Breach Log as required.
3. Data Breach Report. If Staff must report the following details concerning a data breach to the DPO:
 - a. What has happened;
 - b. When and how you found out about the breach;
 - c. The people that have been or may be affected by the breach;
 - d. What you are doing as a result of the breach; and
 - e. Who we should contact if we need more information and who else you have told.
 - f. Any additional information surrounding the incident.
4. Upon receiving a report of a possible data breach the DPO will assess the incident and where appropriate, the DPO must report a data breach to the ICO as soon as possible and certainly within 72 hours of the breach occurring. The DPO may report the breach to the ICO using the phone line 0303 123 1113 or online using the report format on the ICO website.
5. The DPO will consider the breach report and use the following criteria to decide upon the appropriate action:

Table 1; Data Classification Criteria:

Classification	Description
Green	No Impact – information formally made public by school or information which would have no impact on privacy or school reputation if it was to be put into the public domain by any other means.
Amber	Strictly internal or agreed partners – school information which is intended strictly for internal use by staff and agreed partners. Information posing little/no risk to privacy – this could also include names, addresses and pupil numbers that pose little or no risk to privacy.
Red/Official-Sensitive	Health & care personal data – personal data which reveals anything about the health or care arrangements of any individuals or families. This includes details about ethnicity, gender or sexuality. Financial personal data – personal data which reveals anything about the financial circumstances of any individuals or families. Employee & partner personal data – personal data on employees of the school and its partners. This includes details about ethnicity, gender or sexuality. Safeguarding information Impact on health, safety & wellbeing – anything which, if disclosed, would impact on the health, safety and wellbeing of people. This includes details about ethnicity, gender or sexuality. School information which would have a significant impact on the reputation or business of the school if it was seen by non-intended recipient because of commercial, legal, fraud, investigatory or other areas where confidentiality.

Table 2; Incident Grading criteria:

Incident Grading – 1 Negligible	
Any type of incident formally recorded, or something worthy of investigation but is a near miss or false positive where there is only a remote chance of data being readable or which has negligible impact on privacy or school	

Incident Grading 2 - Minor	
Confidentiality	Confirmed or likely loss of personal data or other privacy breach relating to up to 10 individuals that poses low risk to privacy and no H&S impacts (eg just name, address, pupil number at amber level).
Integrity	Confirmed or likely issues relating to integrity of information on <10 staff or pupils such as confused identities, out of date information or records misplaced which causes localised inconvenience or delay.
Availability	Some localised and short lived loss of availability, such as through temp systems failure or disruption of service.

Incident Grading 3 - Moderate	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 10 individuals or any breach of official sensitive information at red level. Likely local media interest or adverse publicity.
Integrity	Issue relating to integrity of information to the extent that the data can no longer be understood or is out of date and could have health, social care and safety or other implications.
Availability	Some disruption to critical services that means information is unavailable causing unacceptable impact and invocation of local team business continuity plans.

Incident Grading 4 - Major	
Confidentiality	Confirmed or likely loss of personal data or privacy breach relating to more than 100 individuals or loss of any sensitive personal data at the red level which is highly likely to affect the H&S of one or more individuals or any privacy breach which because of the high profile nature of the persons affected or other circumstances is likely to lead to national media attention.
Integrity	An integrity issue which means data relating to 100+ staff or pupils is in effect no longer usable or understandable and is likely to impact H&S or key teams in the school.
Availability	Sustained loss of availability of information which has serious impact.

Incident Grading 5 - Extreme	
Confidentiality	Loss of data or privacy breach relating at large scale (eg 100,000+ persons or complete dataset); likely national/international media interest/adverse publicity; prolonged damage and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc.
Integrity	Integrity problem which leads to significant amounts of data on 100k persons being unreadable/unusable and leads to H&S issues or significant service issues.
Availability	Outage or other issue which leads to general failure of IT so that critical areas to the school are not running and business continuity plans are invoked.

Orwell Park School – Staff Privacy Notice**Who We Are**

Orwell Park School Educational Trust Ltd (“the School”) is the data controller for the purposes of data protection law. Contact: DPO@orwellpark.org

Purpose of this Notice

This notice explains how and why the School collects, uses, and shares personal information about our current and former staff. It also explains your rights under data protection law.

What Personal Data We Collect

We collect and use personal data such as:

- Contact details (name, address, phone, email)
- Employment and contract information
- Payroll and pension details
- Qualifications, CVs, references
- Safeguarding and disciplinary records
- Health and welfare information (e.g. medical conditions, absence details)
- DBS and criminal records checks
- IT usage and communication monitoring (as per the IT policy)
- Images (e.g. staff ID, photos in publications or on our website/social media)

Why We Use Your Data

We process your data for purposes including:

- Recruitment and HR administration
- Safeguarding and legal compliance
- Performance management, training and professional development
- Payroll, pensions and tax
- Health and safety, and wellbeing
- IT services and monitoring
- Internal reporting, planning, and auditing
- Legal claims and insurance Some processing is required by law; others are for our legitimate interests in running a safe and effective school.

Sharing Data

We may share your data with:

- Government and regulatory bodies (e.g. HMRC, DfE, ISI)
- Payroll and pension providers
- Insurers, legal or professional advisers
- IT service providers (e.g. cloud-based platforms) We ensure third parties process data securely and only under our instructions.

Retention of Data

Staff records are retained securely for up to 7 years after employment ends, unless a longer period is legally required (e.g. safeguarding).

Your Rights

You have rights under data protection law, including:

- Accessing your data
- Correcting or deleting inaccurate data
- Objecting to or restricting processing
- Data portability in some cases To make a request or raise a concern, contact DPO@orwellpark.org

Keeping Data Secure

We take appropriate technical and organisational steps to protect your data. All staff are required to comply with our Data Protection Policy and complete relevant training.

Updates

We may update this notice from time to time. Substantial changes will be communicated directly where appropriate.

Queries or Complaints

Please contact the DPO in the first instance. If concerns remain unresolved, you may contact the Information Commissioner’s Office (ICO).

Orwell Park School – Pupil Privacy Notice

Who We Are

Orwell Park School Educational Trust Ltd (“the School”) is the data controller for your personal data.

Contact: DPO@orwellpark.org

Purpose of this Notice

This notice explains how and why we collect and use personal information about our current and past pupils.

What Personal Data We Collect

We may collect and use:

- Name, date of birth, contact details
- Admissions, academic and attendance records
- Reports, assessments and exam results
- Medical information, including allergies and conditions
- Behavioural and disciplinary records
- Safeguarding and welfare records
- Special educational needs (SEN) information
- Images (e.g. in school publications, website or social media)
- IT and online activity (e.g. school email, WiFi usage)

Why We Use Your Data

We use this information to:

- Deliver teaching, learning and pastoral care
- Support your wellbeing and development
- Monitor progress and achievements
- Communicate with parents and carers
- Comply with legal obligations (e.g. safeguarding, health and safety)
- Manage trips, activities and events
- Maintain records of your time at school
- Promote the school (e.g. newsletters, social media with appropriate consent)

Some of this use is required by law; other uses rely on our legitimate interests or, where needed, your or your parents’ consent.

Sharing Data

We may share your data with:

- Exam boards, regulators, inspectors (e.g. ISI, DfE)
- Health professionals and support services
- Trip providers or event organisers
- Other schools (e.g. if you move)
- Law enforcement or local authority where required

Retention of Data

Pupil records are kept securely during and after your time at the school. Some records (e.g. safeguarding) must be kept for longer periods by law.

Your Rights

You (or your parents, if you are not old enough) have rights including:

- Accessing your personal data
- Requesting corrections or deletions
- Objecting to how we use your data (where lawful) Contact DPO@orwellpark.org for more information.

Keeping Data Secure

We protect your data with appropriate security and limit access to only those who need it.

Orwell Park School – Parent and Carer Privacy Notice

Who We Are

Orwell Park School Educational Trust Ltd (“the School”) is the data controller. Contact: DPO@orwellpark.org

Purpose of this Notice

This notice explains how we collect, use and share personal data about parents and carers of current, former and prospective pupils.

What Personal Data We Collect

This includes:

- Names, addresses, phone numbers and email addresses
- Financial information (e.g. fee payments, bursary applications)
- Records of correspondence with the school
- Information shared with us for safeguarding or wellbeing purposes
- Occupation and professional details (e.g. for fundraising or alumni engagement)
- Photo or video images taken at school events (with consent where needed)

Why We Use Your Data

We process parent and carer data to:

- Support your child’s education and welfare
- Communicate about school activities, events or matters of concern
- Manage contracts and billing
- Meet safeguarding and legal obligations
- Promote the school and maintain community links (e.g. alumni newsletters)
- Fundraise or seek support for school development (with consent where required)

Sharing Data

We may share your data with:

- Educational authorities, local authorities, regulators (e.g. DfE, ISI)
- Legal and professional advisers
- IT and cloud service providers
- Event or trip organisers, where needed

Retention of Data

Your data is kept securely for as long as needed to support your child or maintain school records. Financial and safeguarding data may be kept longer where legally required.

Your Rights

You have rights including to:

- Access your data
- Ask for corrections or deletions
- Object to marketing or fundraising communications

You may withdraw consent where that is the legal basis for use. Contact DPO@orwellpark.org

Keeping Data Secure

Your information is protected by appropriate security measures and used only for the intended purposes.

Orwell Park School – Alumni and Supporter Privacy Notice

Who We Are

Orwell Park School Educational Trust Ltd (“the School”) is the data controller for the personal data of alumni and supporters. Contact: DPO@orwellpark.org

Purpose of this Notice

This notice explains how we collect, store and use personal information about former pupils (Old Orwellians), past parents and others who support the school.

What Personal Data We Collect

We may collect:

- Contact details (name, email, address, phone number)
- Education and career information
- Attendance at events and school-related activities
- Images (e.g. from events, school publications or newsletters)
- Information from donations or fundraising interactions
- Publicly available data (e.g. professional achievements)

Why We Use Your Data

We use this data to:

- Stay in touch with you
- Send newsletters or updates about the school
- Invite you to reunions, events or talks
- Share information about fundraising campaigns
- Maintain a record of your relationship with the school

Sharing Data

We may share your data with:

- The Old Orwellians association
- Fundraising partners or platforms (where used)
- Professional advisers or IT service providers

Retention of Data

We keep alumni and supporter records securely for as long as the relationship remains active. If you ask us not to contact you, we may retain minimal information to honour your request.

Your Rights

You have the right to:

- Access your personal data
- Correct or update your details
- Object to contact or data use for fundraising

You can update your preferences or withdraw consent by contacting the School Marketing Officer or DPO@orwellpark.org

Keeping Data Secure

We protect all personal data using secure systems and restrict access to authorised personnel only.