Parkstone Grammar School

GENERAL DATA PROTECTION REGULATIONS POLICY

DATE APPROVED	July 2023
APPROVED BY	Finance and Premises Committee
NEXT REVIEW	2023-24
TYPE OF POLICY	Statutory

CONTENTS

1. AIMS AND SAFEGUARDING

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Secure processing of data ensures the safeguarding of individuals' rights and identities.

2. LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. This policy is amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit)) Regulations 2019 which amended the DPA 2018 and merged it with the requirements of the EU GDPR to form a UK specific data protection regime that works post Brexit. This new regime is known as the "UK GDPR".

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

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

3. DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs

	• Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that decides how and why to collect and use data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

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

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

5. ROLES AND RESPONSIBILITIES

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

5.1 Governing Board

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

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

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

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Alan Triplow (School Business Manager) and is contactable via email at alan.triplow@parkstone.poole.sch.uk.

5.3 Headteacher
The headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All Staff
Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school must comply with.
The principles say that personal data must be:

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

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

7. COLLECTING PERSONAL DATA

7.1 Lawfulness, Fairness and Transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent** for a specific purpose

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

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

We will only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified effects on them. We will be clear, open and honest about how and why we use personal data.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the school's Records Management Policy.

8. SHARING PERSONAL DATA

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff. Specifically, during the COVID pandemic, GDPR law allows Public Health England to use the personal data collected by NHS Test and Trace Service. Therefore, if required to do so by NHS Track and Trace, the school will provide the contact details of all children and adults that have been in close contact with anyone that has tested positive with COVID-19 within the setting.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'subject access request' to obtain a copy of their personal data. It helps individuals to understand how and why data is being used by the school and to check it is being used lawfully.

Subject access requests must be submitted in writing, either by letter, or email to the DPO. The preferred format is included at Appendix 2. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

9.2 Children and subject access requests
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request.

9.3 Responding to Subject Access Requests
When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

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

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

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

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

As an Academy there is no automatic parental right of access to the educational record however the school will provide this information provided that the student gives their consent. Requests must be made to the Data Protection Officer by a subject access request.

11. BIOMETRIC RECOGNITION SYSTEMS

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

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners using a 4 digit pin code at each transaction if they wish.

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

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

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

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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

Any enquiries about the CCTV system should be directed to the DPO, Alan Triplow.

13. PHOTOGRAPHS AND VIDEOS

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

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

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

Uses may include:

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

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

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

14. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:

- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.
In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff will ensure secure and sensible transit and storage
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are forced to change their passwords every 90 days.
- Encryption software is used to protect all portable devices and removable media, such as laptops.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours.

18. TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated as necessary and reviewed **every 3 years** and shared with the full governing board.

20. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Freedom of Information Policy
- Records Management Policy
- Child Protection Policy
- ICT Acceptable Use Policies

APPENDIX 1: PERSONAL DATA BREACH PROCEDURE

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO). This must be done in person.

If the DPO is not immediately available you should notify one of the following staff. Please attempt to contact the people listed in order until you make contact with somebody:

- Headteacher
- Deputy Headteacher
- Assistant Headteacher
- Network Manager
- Chair of Governors

- The DPO (or other designated person) will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people.

- The DPO will alert the Headteacher (email) and the chair of governors (via email) of reportable breaches.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure).
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored in the Data Breach folder, and logged on the Data Breach spreadsheet. These are located in a secure folder on the schools IT network.

Where the ICO must be notified, the DPO will do this via the https://ico.org.uk/for-organisations/report-a-breach within 72 hours. As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the Data Breach folder, and logged on the Data Breach spreadsheet. These are located in a secure folder on the schools IT network.

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

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is being emailed it should be done so via ‘secure mail’.
- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

APPENDIX 2 – PRIVACY NOTICE - Staff

This privacy notice describes how we collect and use personal data about staff, in accordance with the UK General Data Protection Regulation (UK GDPR) tailored by the Data Protection Act 2018.

Who collects this data
Parkstone Grammar School is a "data controller", which means we are responsible for deciding how we hold and use personal data about students.

What categories of data might we collect, process, hold and share
We collect and hold some information relating to those that we employ or otherwise engage to work at our school. This may include, but is not restricted to:

- Personal information (such as name, DOB unique staff number and contact/next of kin)
- Characteristics (such as gender, age, ethnic group)
- Contract information (such as start date hours worked, role and salary/pension information)
- Qualifications and performance information
- Work absence information (such as number of absences and reasons)
- Relevant medical information including dietary needs
- Biometric data, photographs or CCTV images
- Information about the use of our IT, communications and other systems
- Financial data (such as bank account)
- Recruitment information (such as copies of right to work, references, driving licence)

Collecting this information
Whilst most information you provide to us is mandatory, some may be voluntary, and we will make it clear when it is voluntary. It is important that personal information we hold about you is accurate and current and please keep us informed of any changes.

Why we use this data
We use the data to help run the school, including, and not restricted to:

- Enable you to be paid
- Facilitate safe recruitment as part of our safeguarding obligations towards students
- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform our recruitment and retention policies
- Support effective performance management
- Allow appropriate curriculum and financial modelling
- To provide data for statistical purposes

The lawful basis on which we use this information
We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and

- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

Storing data
The school keeps information about staff on computer systems and sometimes on paper. Except as required by law, the school only retains information for as long as necessary in accordance with timeframes imposed by law and our internal policy. We have put in place measures to protect the security of your information (against it being accidentally lost, used or accessed in an unauthorised way).

Who we share information with
We do not share information about staff with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about staff with:

- Health and social welfare organisations - to meet our legal obligations to share certain information with them and to carry out our tasks in the public interest;
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and;
- The Department for Education - to carry out our tasks in the public interest, for example to provide information on the workforce census;
- The staff member's family or representatives – to protect the staff's vital interests for example in the case of a medical emergency;
- Educators and examining bodies – to carry out our tasks in the public interest to assess student examination work;
- Our regulator e.g. Ofsted – to meet our legal obligation to be inspected;
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll;
- Our auditors and Responsible Officer – to meet our legal obligation to have our financial accounts audited on an annual basis;
- Police forces, courts, tribunals – to meet our legal obligations to share certain information with it, such as safeguarding concerns.

Requesting Access to Your Personal Data
Under data protection legislation, individuals have the right to request access to information about them that we hold. To make a request for your personal information, contact the Data Protection Officer whose contact details are noted below. This is done using a standard form "subject access request".
You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage/distress;
- Prevent processing for the purposes of direct marketing;
- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the data protection regulations.

If you want to exercise any of the above rights, please contact the Data Protection Officer in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access

the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to Withdraw Consent

In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Contact – Data Protection Officer

If you would like to discuss anything relating to the school's compliance with the General Data Protection Regulation that you have not been able to resolve with the school first, please contact Alan Triplow the Data Protection Officer by email (alan.triplow@parkstone.poole.sch.uk).

Appendix 3 – PRIVACY NOTICE – Students

This privacy notice describes how we collect and use personal data about students, in accordance with the UK General Data Protection Regulation (UK GDPR) tailored by the Data Protection Act 2018.

Who collects this data
Parkstone Grammar School is a "data controller", which means we are responsible for deciding how we hold and use personal data about students.

What categories of data might we collect, process, hold and share
We collect and hold some information about you to make sure we can help you learn and to look after you at school. This may include, but is not restricted to:

- Personal information (such as name, DOB unique student number and contact information)
- Characteristics (such as ethnicity, language, country of birth and free school meal eligibility)
- Attendance information
- Assessment information (internal and external)
- Relevant medical information including dietary needs
- Special educational needs and safeguarding information
- Details of any behaviour issues or exclusions
- Biometric data, photographs or CCTV images
- Information about the use of our IT, communications and other systems
- Financial data

Collecting this information
Whilst most information you provide to us is mandatory, some may be voluntary, and we will make it clear when it is voluntary. It is important that personal information we hold about you is accurate and current and please keep us informed of any changes.

Why we use this data
We use the data to help run the school, including, and not restricted to:

- Support student learning
- Monitor and report on student progress
- Provide appropriate pastoral care and protect student welfare
- Assess performance of the school and quality of our provision
- Security purposes
- Student selection
- Compliance with the law regarding data sharing

The lawful basis on which we use this information
We will only use your information when the law allows us to. Most commonly, we will use your information in the following circumstances:

- Consent: the individual has given clear consent to process their personal data for a specific purpose;
- Contract: the processing is necessary for a contract with the individual;
- Legal obligation: the processing is necessary to comply with the law (not including contractual obligations);
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law; and

- The Education Act 1996: for Departmental Censuses 3 times a year. More information can be found at: https://www.gov.uk/education/data-collection-and-censuses-for-schools.

We need all the categories of information in the list above primarily to allow us to comply with legal obligations. Please note that we may process information without knowledge or consent, where this is required or permitted by law.

Storing data
The school keeps information about students on computer systems and sometimes on paper. Except as required by law, the school only retains information for as long as necessary in accordance with timeframes imposed by law and our internal policy. We have put in place measures to protect the security of your information (against it being accidentally lost, used or accessed in an unauthorised way).

Who we share information with
We do not share information about students with any third party without consent unless the law and our policies allow us to do so. Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about students with:

- Health and social welfare organisations - to meet our legal obligations to share certain information with them, such as safeguarding concerns and exclusions and to carry out our tasks in the public interest for example to facilitate inoculations;
- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions;
- The Department for Education - to carry out our tasks in the public interest, for example to provide information on the student census;
- Other schools that the student has attended or may attend
- The student's family or representatives – to protect the student's vital interests for example in the case of a medical emergency;
- Educators and examining bodies – to carry out our tasks in the public interest to assess student examination work;
- Our regulator e.g. Ofsted – to meet our legal obligation to be inspected;
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as online payments;
- Our auditors and Responsible Officer – to meet our legal obligation to have our financial accounts audited on an annual basis;
- Police forces, courts, tribunals – to meet our legal obligations to share certain information with it, such as safeguarding concerns.

Youth Support Services
Once our students reach the age of 13, we also pass student information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13–19-year-olds under section 507B of the Education Act 1996.

This information enables it to provide youth support services, post-16 education and training services, and careers advisors.

A parent or guardian can request that only their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/student once they reach the age 16.

The National Pupil Database (NPD)
Much of the data about students in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes.

This information is securely collected from a range of sources including schools, local authorities and awarding bodies. To find out more about the NPD, go to https://www.gov.uk/government/collections/national-pupil-database

Requesting Access to Your Personal Data
Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, contact the Data Protection Officer whose contact details are noted below. This is done using a standard form "subject access request".

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent. Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

You also have the right to:

- Object to processing of personal data that is likely to cause, or is causing, damage/distress;
- Prevent processing for the purposes of direct marketing;
- Object to decisions being taken by automated means;
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the data protection regulations.

If you want to exercise any of the above rights, please contact the Data Protection Officer in writing. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

Right to Withdraw Consent
In circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Data Protection Officer. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Contact – Data Protection Officer
If you would like to discuss anything relating to the school's compliance with the General Data Protection Regulation that you have not been able to resolve with the school first, please contact Alan Triplow the Data Protection Officer by email (alan.triplow@parkstone.poole.sch.uk).