Poole High School

VALUED • INSPIRED • EMPOWERED

Data Handling Policy

Staff Link:	P Myers	**Date:**	July 2021
Governor Link:	P Woodroffe	**First Review:**	July 2023
		Subsequent Reviews:	Bi-annual

Contents

1. Aims

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 UK data protection law.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the:

- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)

It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

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

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

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

Term	Definition
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 determines the purposes and the means of processing of personal 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 with the ICO (registration number Z890387X and has paid its data protection fee to the ICO, as 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 even in a voluntary capacity. 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 in school is the Head of IT and Data Security and is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our external DPO is Handsam Ltd and is contactable via info@handsam.co.uk

The members of staff responsible for day to day matters relating to Data Protection are the Head of IT and Data Security and Director of Finance and Operations.

5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis but may delegate this to other members of staff (Head of IT and Data Security or Director of Finance and Operations).

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 UK 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 or another person i.e. 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 or exercise its official authority**

- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

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.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 record retention schedule.

The information we collect will include:

Personal information about members of the school community:

For students we collect and process data relating to the students on roll (and formerly on roll). This information will include their

- contact details,
- national curriculum assessment results,
- attendance information,
- any exclusion information,
- where they go after they leave us,

and personal characteristics such as their

- ethnic group,
- any special educational needs
- relevant medical information.

For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.

8. Sharing personal data

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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 UK data protection law
    - Establish a contract with the supplier or contractor 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

A list of data processing subcontractors can be found in appendix B

We will also share personal data with law enforcement and government bodies where we are legally required to do so. For example, we are required, by law, to pass some information about our students to the Department for Education (DfE). This information will, in turn, then be made available for use by the Local Authority.

The DfE may also share student level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the UK GDPR from May 2018.

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.

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

- https://poole.gov.uk (Our local authority)
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data (DfE)

If you are unable to access these websites, please contact the DfE as follows: Public Communications Unit, Department for Education, Sanctuary Buildings, Great Smith Street, London SW1P 3BT

For staff members we collect and process data which will include their

- Personal details such as
  - names,
  - addresses,
  - contact details,
  - contact details,
  - disciplinary records
- Professional records e.g.
  - employment history,
  - training
  - taxation and national insurance records,
  - appraisal records
  - absence Information
  - references

See Appendix C for a list of additional data processing subcontractors for staff.

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 gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

If staff receive a subject access request in any form 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. Therefore, most subject access requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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 (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it.

This right applies as long as the pupil concerned is aged under 18.

There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11. 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 Peter Myers (Head of IT and Data Security) or David Newman (Director of Finance and Operations).

12. 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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

Where the school takes photographs and videos, 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 photographers, newspapers, campaigns

- Online on our school website or social media pages
    - We will seek specific consent for each type of use in our data collection forms issued when a student joins the school

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will remove the use of 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.

13. Data protection by design and default

We have 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. The school has retained Handsam Ltd to act in this capacity. Most matters will be dealt with internally by the in-school data protection officer and referred on to Handsam Ltd if required either for severity or expertise.
- 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 data protection 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
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure

14. 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 stored securely when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

- Passwords that are at least 7 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- 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 ICT 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)

15. 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 students this will be at the end of the school year in which they would have obtained the age of 25 (DOB +7 years.). We will retain a list of when records were deleted.

For example, we will shred 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.

16. 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 after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

17. 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.

18. Monitoring arrangements

The Head of IT and Data security is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and approved by the full governing board.

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- ICT Acceptable Use Policy

- CCTV Policy and Code of Practice
- Safeguarding Policy

Appendix A: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by email.
- The school will undertake an initial investigation and report to the ICO and DPO is it is deemed necessary. This will be by the data protection officer in school. The investigation will consider the breach report and determine whether a breach has occurred. To decide, it 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
    - If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
    - The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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) before and after the implementation of steps to mitigate the consequences
    - The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool
    - The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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

- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 our Breach Record Form
- 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
- The DPO and headteacher will meet termly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

- We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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 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 IT Support Team to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
        - In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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 endeavour to obtain 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
    - Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked, and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Appendix B: Data Processors working on behalf of Poole High School

This list represents a snapshot from when the policy was written and is indicative of the types of companies data is shared with for the purposes of providing a service. This list is only updated when the policy is reviewed, and a current list is available on request.

Data Processor	Reason	Information shared.
Megaseatingplan	To provide login details for staff Facilitate tracking and classroom management	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information
Capita SIMS – our Management Information System providers.	To provide login details For resolving issues.	Parent names and related student information are provided to create logins. Under normal circumstances they have no access to personal data but may be allowed access in the event of a problem with the Management Information system. In this case, this is carried out over an encrypted link and data is retained only so long as it is needed to resolve the issue.
Google – providers of email and online storage system	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
GCSEPod	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
Kerboodle	To provide login details	Name, DoB, Class Information.
Wonde	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information
GroupCall	To transfer data to other processors. They are a conduit but do not actually do any processing of the data.	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, EAL and Child in Care information
School Cloud Systems	To facilitate the arrangement and booking of Parents' Evenings.	Name, DoB, Class Information, Year Group, Parent Name and Email
Wisepay	To provide login details and allow online payments	Name, Year Group, Class Information, Parent Name and Contact Details
Sharp Retail Systems	To Provide our cashless catering system	Name, Year group, class information, dietary requirements and allergies, account balance.
Flash Academy **Hegarty Maths** **Reading Cloud** **Project Q** **Dynamic Learning** **Careers Start Profile**	To provide login details	Name, DoB, Class Information.

Appendix C: Data Processors working on behalf of Poole High School for Staff Specific Data

This list represents a snapshot from when the policy was written and is indicative of the types of companies data is shared with for the purposes of providing a service. This list is only updated when the policy is reviewed and a current list is available on request.

Data Processor	Reason	Information shared.
Dorset Payroll	To provide payroll services	Name, Bank details,
SBS	For HR and consultancy	Name, PayScale, hours worked, employee number, start date, dates for maternity leave (if applicable), leaving date.
Occupational Health	Ad hoc	Name, reason for referral
Potential Future employers	References	Name, Current Position, attendance summary, performance summary, safeguarding information.
Triptico	To provide login details	Name

Poole High School
VALUED • INSPIRED • EMPOWERED

GDPR Privacy Notice (Students and Parents)

Introduction.

Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. Access to data is restricted so that only members of the school community who need access will be able to access it. This notice serves to explain what we are collecting, why we are collecting it and how it will be stored.

Why we are collecting information relating to students.

This information is being collected for the purpose of planning and provision of education services for the student. We collect this because it is necessary to carry out the education services in the public interest and it forms part of the contract between home and school. We retain information about students until they reach the age of 25 (in line with suggested guidelines for data retention in schools) for the purposes of providing references and verification of exam results.

Commented [PM1]: Need to make sure we are clear on what we may and may not do here.

There are some pieces of information we would like to collect but are not essential to providing an education so for these we will seek your consent. These will be signposted where relevant.

Personal Data

The school will have access to a wide range of personal information and data. The data may be held in digital format or on paper records.

The information we collect will include:

Personal information about members of the student body:

- For students we collect and process data relating to the students on roll (and formerly on roll).This information will include their
  - Full and preferred names.
  - Date of Birth.
  - contact details.
  - national curriculum assessment results,
  - attendance information,
  - any exclusion information,
  - where they go after they leave us

  and personal characteristics such as their
  - ethnic group,
  - any special educational needs
  - relevant medical information.
  -
  -

For students enrolling for post 14 qualifications, the Learning Records Service will give us the unique learner number (ULN) and may also give us details about their learning or qualifications.

Once our students reach the age of 13, the law requires us to pass on certain information to the Borough of Poole or the Youth Support Services in the area who have responsibilities in relation to the education or training of 13-19 year olds. We may also share certain personal data relating to young people aged 16 and over with post-16 education and training providers in order to secure appropriate services for them.

A parent/guardian can request that **only** their child's name, address and date of birth be passed to Borough of Poole or Youth Support Services by informing the school. This right is transferred to the young person once he reaches the age of 16. For more information about services for young people, please go to our local authority website at www.poole.gov.uk/communities-and-people/youth-support/youth-service.

Commented [PM2]: Not sure whether this will remain

The DfE conducts school census three times a year and we share data as required for this purpose.

Commented [PM3]:

We share data (for the purposes of providing systems) with the following companies as data processors. In principle the purposes of these systems are to support the core principles of the school by providing accounts and tracking progress.

System/Company	Reason	Information shared.
E-praise.co.uk	To provide login details Facilitate tracking and classroom management	Name, DoB, Class information, House, Gender, UPN, Year Group, AEN, Pupil Premium, Child in Care and EAL information
Realsmart – our VLE providers	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
Capita SIMS – our Management Information System providers.	To provide login details For resolving issues.	Parent names and related student information are provided to create logins. Under normal circumstances they have no access to personal data, but may be allowed access in the event of a problem with the Management Information system. In this case, this is carried out over an encrypted link and data is retained only so long as it is needed to resolve the issue.
Google – providers of email and online storage system	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
GCSEPod	To provide login details	Name, Year Group, Class information, House, UPN, Year Group.
Accelerated Reader	To provide login details	Name, DoB, Timetable information, Ethnicity, AEN
Kerboodle	To provide login details	Name, DoB, Class Information.
Fraser Portraits	To provide	Name, Admission Number and Registration Class

Commented [PM4]: Spoke to these guys yesterday (5/6/17.
Aware of gdpr but highlighted that they in turn use a number of data processors. Servers and emails

	photography services for the school.	
Wonde		
GroupCall		

We will not give information about our pupils to anyone without your consent (as indicated via the Data Collection Form parents/guardians complete on entry to the school) unless the law and our policies allow us to do so.

The School may hold the information that you provide in both computerised and manual record systems. The information you provide may also be disclosed to the DfE; courts and tribunals should the appeal become the subject of dispute. Information will be held and used in compliance with the GDPR.

You are able to see a copy of the information held about you on application to the School's Data Protection Officer. For further information about access please contact the school and ask to speak to the data protection officer.

GDPR Privacy Notice (Contractors)

Introduction.

The General Data Protection Regulation (GDPR) is the development of the Data Protection Act (1998) and will come into effect on the 25th May 2018. It covers all the countries in the EU and will be adopted by the UK. Although based on the Data Protection Act 1998 it means schools will have to change their approach to Data Protection.

GDPR changes the importance of looking after the data we have about you and making sure we keep it safe so no-one can misuse it.

This notice is to help you understand how and why we collect your personal data and what we do with that data. It also explains the decisions that you can make about your own data.

Poole High School is classed as the data controller. This means the school determines the purpose for which, and the manner in which, any personal data is to be processed. Any combination of data items that identifies an individual and provides specific data about them, their families or circumstances is considered to be personal data.

Why do we collect your personal data?

In order to manage your application, we may need to process certain personal data about you. We only process your data as necessary for the purposes of pursuing your application or as required by law or regulatory requirements, so not all of the purposes set out below will apply to you all of the time.

Data supplied on the application form (name, employment company, contact details) will be used to communicate with you and ensure the safety of .

Personal data about you collected during the interview process (including notes made during face to face, telephone or video interviews), teaching assessments or technical assessments will be used to make a decision on candidate selection.

Criminal records checks

All applicants for positions at Poole High School are subject to an enhanced DBS clearance check. Data provided as part of the application will be used to make this check, consisting of name and email address. We will in due time receive clearance or otherwise from the Disclosure and Barring Service.

What personal data is processed?

We will have access to a range of data during the application process, including:

- Personal details such as name;
- Company Details, such as name, telephone number and email address.
- Video from on site CCTV. (This will be dealt with under the terms of our CCTV policy)

If you are visiting the site, then we may also capture some sensitive personal data about you (e.g. disability data). We do this in order to make reasonable provision for you on site.

Who do we share your personal data with?

The school will only share your details externally in the event that there is a dispute or need for the authorities or police to be called. In these cases only relevant details to the situation will be shared.

How do we protect your data?

All data collected is protected to ensure that unauthorised or unlawful processing of personal data, accidental loss or destruction of, or damage to, personal data does not occur.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to data about you that we hold. To make a request for your personal data, please email school@poolehigh.poole.sch.uk and ask to make a subject access request and state what data you require. Alternatively, there is data available on our website about accessing your personal data, please visit http://poolehigh.co.uk/data-protection.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose 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 have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Data Commissioner's Office at https://ico.org.uk/concerns/

Other Important Documents.

This privacy notice should be used in conjunction with the Data Protection Policy and CCTV Policy which can be found on our website: https://poolehigh.co.uk/about/policies/ .

GDPR Privacy Notice (Job Applicants)

Introduction.

The General Data Protection Regulation (GDPR) is the development of the Data Protection Act (1998) and will come into effect on the 25th May 2018. It covers all the countries in the EU and will be adopted by the UK. Although based on the Data Protection Act 1998 it means schools will have to change their approach to Data Protection.

GDPR changes the importance of looking after the data we have about you and making sure we keep it safe so no-one can misuse it.

This notice is to help you understand how and why we collect your personal data and what we do with that data. It also explains the decisions that you can make about your own data.

Poole High School is classed as the data controller. This means the school determines the purpose for which, and the manner in which, any personal data is to be processed. Any combination of data items that identifies an individual and provides specific data about them, their families or circumstances is considered to be personal data.

Why do we collect your personal data?

In order to manage your application, we need to process certain personal data about you. We only process your data as necessary for the purposes of pursuing your application or as required by law or regulatory requirements, so not all of the purposes set out below will apply to you all of the time.

Data supplied on the application form (name, address, employment history, academic and professional qualifications, gender) will be used to communicate with you and decide on your suitability for interview.

Personal data about you collected during the interview process (including notes made during face to face, telephone or video interviews), teaching assessments or technical assessments will be used to make a decision on candidate selection.

Criminal records checks

All applicants for positions at Poole High School are subject to an enhanced DBS clearance check. Data provided as part of the application will be used to make this check, consisting of name and email address. We will in due time receive clearance or otherwise from the Disclosure and Barring Service.

What personal data is processed?

We will have access to a range of data during the application process, including:

- Personal details such as name, address, date of birth;
- Work history; previous employers, positions, dates, etc.
- Salary,
- Education and work history including professional qualifications and skills;
- References
- Nationality / visa / right to work permit data; (e.g. passport, driving licence, National Insurance numbers)
- Assessment results e.g. interview, lesson observation or technical tasks.
- Video from on site CCTV. (This will be dealt with under the terms of our CCTV policy)

During the process we may also capture some sensitive personal data about you (e.g. disability data). We do this in order to make reasonable adjustments to enable our candidates to apply for jobs with us to attend interviews, to prepare for starting at the school (if successful) and to ensure that we comply with regulatory obligations placed on us with regard to our recruitment.

Who do we share your personal data with?

The school will need to share your personal data with members of the selection panel, and other members of staff involved in the recruitment process including HR staff. Other members of staff will not have access to your data.

How do we protect your data?

All data collected is protected to ensure that unauthorised or unlawful processing of personal data, accidental loss or destruction of, or damage to, personal data does not occur. All unsuccessful applications are held in secure storage for 6 months after the date of interview. Successful applications will form part of your employment record.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to data about you that we hold. To make a request for your personal data, please email school@poolehigh.poole.sch.uk and ask to make a subject access request and state what data you require. Alternatively, there is data available on our website about accessing your personal data, please visit http://poolehigh.co.uk/data-protection.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose 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 have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Data Commissioner's Office at https://ico.org.uk/concerns/

Other Important Documents.

This privacy notice should be used in conjunction with the Data Protection Policy and CCTV Policy which can be found on our website: https://poolehigh.co.uk/about/policies/ .