Data Protection Policy

Park Community School

Adopted by PCE Ltd and PCV (Charity)

The purpose of this policy is to set out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

Contents

Introduction
The school collects and uses personal information (referred to in the General Data Protection Regulation (GDPR) as personal data) about staff, students, governors, parents, visitors and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

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

The school is the Data Controller, of the personal data that it collects, receives and processes for these purposes. The school is registered with the ICO and has paid its data protection fee as legally required.

The school has a Data Protection Officer, Jamie Bryce, who may be contacted at dpo@pcs.hants.sch.uk

The school issues Privacy Notices (also known as a Fair Processing Notices) to all students/parents and staff (see Appendices 1 and 2). These summarise the personal information held about students and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data

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 UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

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 guidance 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.

Roles and responsibilities
This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information regardless of how it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

Governing Body has overall responsibility for ensuring that our school compiles with

all relevant data protection obligations.

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 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 Jamie Bryce and is contactable via dpo@pcs.hants.sch.uk

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

All 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

What is Personal Information/data?
Personal information or data means any information relating to an identified or identifiable living individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, employee/payroll number, location data, an online identifier (i.e. user name) or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Special categories of personal data which is more sensitive and therefore needs more protection is information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

Data Protection Principles
The UK GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)
3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive
4. Personal data shall be accurate and where necessary, kept up to date
5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6. Personal data shall be processed in a manner that ensures appropriate security of the personal

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

Collecting personal data
Lawfulness, fairness and transparency:

- We will only process personal data where we have 1 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 student) 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 student) 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 student) 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.

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.

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 student 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 students – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that 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
- We will also share personal data with law enforcement and government bodies where we are legally required to do so
- 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 students or staff
- Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

Subject access requests and other rights of individuals

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 must be 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.

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 students at our school may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Responding to subject access requests
When responding to requests, we:

- We will 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 (20 school days) of the request (or receipt of the additional information needed to confirm identity, where relevant)
- There will be a cost for the processing of the information
- 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 student or another individual
    - Would reveal that the student is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the student'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.

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, 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 that 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.

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 student) 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 student 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 student or another individual, or if it would mean releasing exam marks before they are officially announced.

Biometric recognition systems
We use a students' biometric data as part of an automated biometric recognition system for use of accessing school food, photocopier use and laptops. We will comply with the requirements of the Protection of Freedom Act 2012.

Parents/carers are requested to give written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers can withdraw consent at any time and we will make sure that any relevant data already captured is deleted.

When staff members or other adults use the school's biometric system we will also obtain their consent before they first take part in it. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

Use of CCTV
We use CCTV in various locations around the school site to ensure it remains safe.

We will follow the ICO's guidance for the use of CCTV and comply with data protection principles. CCTV recordings are not routinely retained for more than 30 days.

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 Facilities Manager.

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 for photographs and videos to be taken of students under 18 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 the student. Where we don't need parental consent, we will clearly explain to the student 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 students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Artificial Intelligence (AI)
Artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Park Community School recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, Park Community School will treat this as a data breach, and will follow the personal data breach procedure.

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, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and students 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, students 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 [e-safety policy / 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

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.

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 5.

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 students

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.

Monitoring arrangements
The DPO is responsible for monitoring and reviewing this policy.

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

Note: the annual review frequency here reflects the Department for Education's recommendation in its advice on statutory policies.

Duties
Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA), unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment
The school is committed to always maintaining the principles and duties in the GDPR. Therefore, the school will:

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this
- If the school plans to transfer personal data outside the EEA, the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.
- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely
- Share personal information with others only when it is legally appropriate to do so
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests)
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards

- Ensure that all staff and governors are aware of and understand these policies and procedures.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to the handling of personal information may be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years. The policy review will be undertaken by the Data Protection Officer, Headteacher, or nominated representative.

Contacts
If you have any enquires in relation to this policy, please contact the Data Protection Officer, who may be contacted at dpo@pcs.hants.sch.uk

Document Control Table	
Associated Documents	Data Breach Policy E-Safety Policy Staff IT Policy Complaints Policy
Date Approved by governors	26/02/2025
Date of Review	February 2028

Appendix 1 – Park Community School Privacy Notice: For those engaged to work or volunteer at the school

This document explains how we use school workforce information:

The categories of school workforce information that we collect, process, hold and share include

- personal information (such as name, previous names, employee or teacher number, national insurance number)
- addresses and contact numbers including next of kin
- special categories of data including characteristics information such as gender, age, ethnic group
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught) and including pre-employment checks
- relevant medical information
- payroll information, e.g. bank details
- car insurance information [to establish adequate insurance for business purposes]
- DBS (Disclosure and Barring Service) check certificate number and disclosure date

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- ensure safeguarding of students

The lawful basis on which we process this information

The lawful basis for collecting and using workforce information for general purposes includes, for example:

For personal data

- performance of a contract with the data subject (member of staff)
- compliance with a legal obligation and/or protection of vital interests e.g. for DBS checks and maintenance of the Single Central Register for student safeguarding.
- performance of public interest tasks, includes educating students on behalf of the Department for Education (DfE) and would therefore include performance management and continuing professional development (CPD) information [note that this, for example, would also come under 'performance of a contract']
- the use of CCTV is also covered by performance of public interest tasks.
- consent would normally only apply to staff photographs/images if used for marketing purposes and to staff business cards.

For special category data (sensitive personal data, including, for example, biometric data)

- necessary and authorised by law for employment obligations

- protect vital interest where consent not feasible
- necessary for establishing, exercising or defence of legal rights
- substantial public interest
- explicit consent (reference GDPR Act 25 April 2018 as well as the Education Act Schools: statutory guidance - GOV.UK (www.gov.uk))

Collecting this information
Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information
We hold school workforce data indefinitely in accordance with Local Authority latest current guidelines.

Who we share this information with
We routinely share this information with:

- our local authority (LA)
- the Department for Education (DfE)

Covid-19 Saliva Testing in School
Should Covid-19 or similar viruses occur we will follow all local authority and government guidelines to minimise or suppress the spread of the virus. Should testing be requested this will be undertaken.

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority
We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)
We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment.

We are required to share information about our school employees with our local authority (LA) and the Department for Education (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools, and all special schools including Student Referral Units and Alternative Provision). All state

funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the DfE including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The DfE may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact the department: https://www.gov.uk/contact-dfe

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact dpo@pcs.hants.sch.uk (the Data Protection Officer – Mr J Bryce, and the data team)

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 Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If you would like to discuss anything in this privacy notice, please contact:
Mr J Bryce, Data Protection Officer

Appendix 2 - Park Community School Privacy Notice for Parents and Students

This document explains how we use our students' personal information.

Why do we collect and use personal information?

We collect and use personal information:

- To support student learning (including with GDPR compliant providers of external online web applications e.g. Sims, Seneca Learning, Hegarty Maths, Classcharts, EduKey, Google packages, Microsoft packages
- To monitor and report on student progress
- To provide appropriate pastoral care and career guidance
- To assess the quality of our services and how well our school is doing
- For statistical forecasting and planning
- To comply with the law regarding data sharing

The categories of personal information that we collect, hold and share include:

- Personal information (such as name, unique student number and address, parent email address and telephone number, emergency contact)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons) and exclusions
- Assessment information
- Modes of travel
- Relevant medical information
- Special educational needs information
- Exclusions / behavioural information
- Post 16 learning information (e.g. destination)
- Looked after child (LAC) status
- Student pupil premium status

The General Data Protection Regulation allows us to collect and use student information on the following basis: with consent of the individual/parent, where we are complying with a legal requirement, where processing is necessary to protect the vital interests of an individual or another person and where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

When the personal information is Special Category Information we may rely on processing being in the substantial public interest in addition to consent of the individual/parent and the vital interests of the individual or another.

Our requirement for this data and our legal basis for processing this data includes the Education Act 1996, 2002 and 2011, The Childrens Act 1989 and 2004, Education and Skills Act 2008, Schools Standards and Framework Act 1998 and the Equalities Act 2010. (See also Article 6 for Personal Data and Article 9 for Special Category Data from the GCPD May 25th 2018)

Most of the personal information you provide to us is mandatory. For example: names, contact details, relevant medical information, special educational needs, attendance information, free school meal eligibility and photographs for use on our management information system (MIS.)

Information is also passed on to us from previous schools, including, for example: assessment, attendance and behaviour data. However, some information provided to us is done so on a voluntary basis.

To comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain personal information to us or if you have a choice in this. This is done through the Park Community School Parental Consent Policy Document, available in hardcopy from reception and online on our website www.pcs.hants.sch.uk/forms.php . Information for which we need your consent includes, for example: biometric data, the taking of students' images for publication e.g. on the school's website and trips where information will need to be passed onto an external company. Where we are using your personal information only on the basis of your consent you may ask us to stop processing this personal information at any time.

Storing personal data
We keep information about students and their parents on computer systems and sometimes on paper.

We hold education records securely and retain them in accordance with the Retention Schedule after which they are destroyed.

Who do we share student information with?
We routinely share student information with:

- Schools/colleges
- Our local authority (including social services, court and police)
- The Department for Education (DfE)
- NHS (e.g. CAHMS)

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

Covid-19 and other viruses
Should Covid-19 or alternative viruses start we see testing being of great value to reduce the transmission. Park Community School (PCS) will follow guidelines produced by both Local Authority and Department of Education.

Why we share student information
We do not share personal information with anyone without consent unless the law and our policies allow us to do so.

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy

and monitoring.

We are required to share information about our students with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Students) (England) Regulations 2013.

Data collection requirements:
To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

What is different about students aged 13+?
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 enables them to provide services as follows:

- youth support services
- careers advisers

A parent / 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 he/she reaches the age 16.

The National Student 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.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the student information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third

parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

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, or be given access to your child's educational record, contact the Data Protection Officer.

You also have the right, subject to some limitations 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, you should raise your concern with us in the first instance or directly to the

Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:
If you would like to discuss anything in this privacy notice, please contact:

dpo@pcs.hants.sch.uk (The Data Protection Officer and team)

Appendix 3 – Park Community School Privacy Notice for Clients

- Park Community Services
- Park Community Enterprises Ltd (PCE)
- Park Community Ventures
- Park Community Catering

We are committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all clients to whom we provide paid services.

Park Community School is a "data controller" for all the organisations listed above. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information. We may amend this notice at any time.

Data protection principles

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

The kind of information we hold about you

Personal data, or personal information, means any information about an individual from which that person can be identified.

We will collect, store, and use the following categories of personal information about you where applicable:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses, qualifications and public liability insurance cover, membership details and constitutions of organisations.
- Name of child if appropriate e.g. for party bookings
- Bank account details
- CCTV footage

The legal basis for holding this information

The legal basis for holding this information is that it is necessary for us to fulfil the contract we have with you when you are purchasing a service from us and where processing is necessary for the performance of a task carried out in the public

interest or in the exercise of official authority vested in the controller. Where the data is used by us to market products or services to you then we will require your consent (see paragraph below.)

How is your personal information collected?
We collect personal information about your service requirements through community booking form, PCE order form, club constitutions, certificates, telephone orders, catering orders, emails and verbally.

How we will use information about you
We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to perform the contract, we have entered into with you
- Where we need to comply with a legal obligation
- Where it is necessary for our legitimate interests (or those of a third party, for example auditors or our insurance companies) and your interests and fundamental rights do not override those interests

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests)
- Where it is needed in the public interest or for official purposes

If you fail to provide personal information
If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our staff).

Change of purpose
We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Consent
We would like to be able to keep you up to date with marketing information such as new services that become available and offers that we may wish to make available to you. For this we would need your consent. This is obtained by your completion of the consent section on the booking form / initial enquiry form.

You have the right to withdraw this consent in writing at any time, through emailing pdp@pcs.hants.sch.uk and/or bookings@pcs.sch.uk

Data sharing
We may have to share your data with third parties, including third-party service

providers, where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so. This might include for example auditors or our insurance company or the police. In each case your interests and fundamental rights do not override those interests.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies and the law. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

Security
We have appropriate security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Data retention
We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

Rights of access, correction, erasure, and restriction
It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

Under certain circumstances, by law you have the right to:
- Request access to your personal information (commonly known as a "data subject access request")
- Request correction of the personal information that we hold about you
- Request erasure of your personal information
- Object to processing of your personal information
- Request the restriction of processing of your personal information
- Request the transfer of your personal information to another party

Contact
For further information about your rights, or if you have any questions about this privacy notice or how we handle your personal information, please contact pdp@pcs.hants.sch.uk and/or bookings@pcs.sch.uk

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

Appendix 4 – Park Community School Privacy Notice for Job Applicants

This Privacy Statement is published by Park Community School.

By submitting your application or your CV, you acknowledge having read and understood this Privacy Statement. If you do not wish your information to be used as follows, please do not submit your application or your CV.

This Privacy Statement sets out:

- which personal data we gather in the course of the application and recruiting process
- how we use your personal data
- who has access to your personal data
- how long we keep your personal data
- how you can access and modify the personal data we collect about you
- how we secure your personal data
- how you can submit questions and remarks

Which personal data do we collect?

This Privacy Statement relates to all personal data that we receive from you and that we collect and process about you in the context of your application and the resulting recruitment process.

The personal data includes: identification and contact details, personal characteristics (such as gender and date of birth), education and work experience (including results, certificates, degrees, references), job preferences, financial data (e.g. current and desired salary), all data in your CV and cover letter, all publicly available data from your LinkedIn profile and other social media or public websites, and all other personal data you have provided to us orally or in writing in the context of your application.

How do we use your personal data?

Your personal data will be used in the context of your application and recruitment process, including for:

- evaluating your skills, qualifications, and interests against our career opportunities
- checking your data, your references and/or conducting background checks (where applicable)
- communication concerning the recruitment process and your application
- implementing improvements to the organisations' application and recruitment process
- The processing for the purposes 1, 2 and 3 described above are necessary for a potential employment contract and the processing for purpose 4 is based on the legitimate interest of the organisation to improve its processes on the basis of your application and recruitment procedure.

Who has access to your personal data?

Your personal data can be shared with Hampshire County Council and if needed with other affiliates of Hampshire County Council. Within these entities, the following staff members have access to your data:

- staff members of the HR department

- recruiting manager
- senior management

In certain cases, technical staff members may have access to your personal data, but only insofar this is necessary to ensure the proper functioning of our technical systems.

The organisation may make use of external service providers or third parties for any of the purposes described above (e.g. recruitment websites or agencies conducting background checks). In such case, access to your personal data will be limited to the purposes described in this Privacy Statement, and in accordance with the requirements of the applicable data protection legislation.

How long do we retain your personal data?
If your application is not successful, we will retain your personal data for a maximum period of 6 months unless we have your explicit consent to hold it for longer.

If your application is successful, your personal data obtained in the context of the application and recruitment procedure will be included your personnel file. You will then be informed separately of how the organisation processes personal data of personnel.

Appendix 5: 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 emailing dpo@pcs.hants.sch.uk and completing a Data Breach Reporting Form. Often speed is of the essence. Form is attached.

The DPO 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

Staff and governors will co-operate 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. Documented decisions are stored online password protected and hard copies within a lockable cabinet.

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 securely.

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 regularly half 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 ICT department 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other breaches could be:

- 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

Data Breach Reporting Form

The aim of this document is to ensure that, in the event of a security incident such as personal data loss, information can be gathered quickly to document the incident, its impact and actions to be taken to reduce any risk of harm to the individuals affected.

The checklist can be completed by anyone with knowledge of the incident. It will need to be submitted and reviewed by the Data Protection Officer who can determine the implications for the school, assess whether changes are required to existing processes and notify the ICO / data subject where appropriate.

SUMMARY OF INCIDENT	
Data and time of incident	
Nature of breach (e.g. theft/ disclosed in error/ technical problems)	
Give a full description of how breach occurred	
PERSONAL DATA	
Give a full description of all the types of personal data involved with the breach but not specifically identifying the individual concerned (e.g. name, addresses, health information etc.)	
How many individuals are affected?	
Have the affected individuals been informed of the incident?	
Is there any evidence that the personal data involved in this incident has been further disclosed?	

If so, please provide details	
IMPACT OF INCIDENT	
What harm is foreseen to the individuals affected? (e.g. could the breach increase the risk of identity theft?)	
What measures have been taken to minimise the impact of the incident?	
Has the data been retrieved or deleted? If yes, state when and how	
REPORTING	
Who became aware of the breach?	
How did they become aware of the breach?	
Form Completed by	
Position	
Date	

Governance and Information Law Team
Hampshire Legal Services
October 2017