Date: 02/10/22

Date for Review: 02/10/24

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

Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. 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. In addition, this policy complies with our funding agreement and articles of association.

Roles and responsibilities

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

CEO

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

All staff

Staff are responsible for:

• Collecting, storing, and processing any personal data in accordance with this policy

• Informing The Playscheme of any changes to their personal data, such as a change of address

• Contacting the CEO 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 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.

Data protection principles

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

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

This policy sets out how The Playscheme aims to comply with these principles.

Collecting personal data

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 Playscheme can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering a contract
- The data needs to be processed so that the Playscheme can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life
- The data needs to be processed so that the Playscheme, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the Playscheme 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 which are set out in the GDPR and Data Protection Act 2018.

    - If we offer online services to pupils, such as tutoring, and we intend to rely on consent as a basis for processing, we will get parental consent.

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with GDPR policy/guidance.

Sharing personal data

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

- There is an issue with a child 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 children – for example, IT companies. When doing this, we will:

Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law. Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share. Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us. We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided. We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our children or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with 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 Playscheme 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
- 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 Subject access requests should include:
- Name of individual

• Correspondence address

• Contact number and email address

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 below the age of 12 are generally not 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 The Playscheme may be granted without the express permission of the pupil. This is not a rule and the child'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:

• May ask the individual to provide 2 forms of identification

• May contact the individual via phone to confirm the request was made

• Will respond without delay and within 1 month of receipt of the request • Will provide the information free of charge

• May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

• Might cause serious harm to the physical or mental health of the pupil or another individual

• Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests

• Is contained in adoption or parental order records

• Is given to a court in proceedings concerning the child If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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, or object to the processing of it (in certain circumstances)

• Prevent use of their personal data for direct marketing

• Challenge processing which has been justified on the basis of public interest

• Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

• Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)

• Prevent processing that is likely to cause damage or distress

• Be notified of a data breach in certain circumstances

• Make a complaint to the ICO

• Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances) Individuals should submit any request to exercise these rights to the CEO.

If staff receive such a request, they must immediately forward it to the CEO.

Parental requests to see the children's records, or those with parental responsibility, have a legal right to free access to their child's record (which includes most information about a pupil) within 15 days of receipt of a written request.

CCTV

We use CCTV in various locations around The Playscheme site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to the CEO- Christopher Young.

Photographs and videos. As part of our Playscheme activities, we may take photographs and record images of individuals within our Playscheme. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and child. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used. Uses may include: • Within the Playscheme on notice boards and in school magazines, brochures, newsletters, etc. • Outside of The Playscheme by external agencies such as a photographer, newspapers, campaigns • Online on our website or social media pages.

Consent can be refused or withdrawn at any time.

If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See our [child protection and safeguarding policy] for more information on our use of photographs and videos.

Data protection

• 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

• Completing privacy impact assessments where the Playscheme's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies

• 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

• Maintaining records of our processing activities, including:

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

Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular: • Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

• Where personal information needs to be taken off site, staff must inform the CEO.

• Passwords that are at least 8 characters long containing letters and numbers are used to access computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

• 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.

Personal data breaches

The Playscheme 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 report the data breach to the ICO within 72 hours. Such breaches may include but are not limited to: • information being made available to an unauthorised person • The theft of a Playscheme laptop containing non-encrypted personal data about children.

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 CEO is responsible for monitoring and reviewing this policy. This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed every 2 years and shared with the full governing board. robust processes or providing further training for individuals) Records of all breaches will be stored.