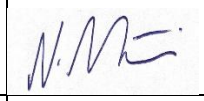
Joy Lane Primary Foundation School

Data Protection Policy

Draft Prepared:	October 2025
Date Agreed:	18th November 2025
Signed by Executive Headteacher: **Ms D Hines**	
Signed by Chair of Governors: **Mrs N Mattin**	
Date Policy to be Reviewed:	November 2026

Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents and carers, 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.

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 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.

Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individuals: › 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.

TERM	DEFINITION
Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), were used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing 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 accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The data controller

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

The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

At Joy Lane we use ClassDojo to communicate with parents and share information. This data is controlled by ClassDojo, not the school. Parents agree to the privacy policy when they sign up on the website/app. Please see the Class Dojo Privacy Policy for any information regarding this.

Roles and responsibilities

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

Governing board

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

Data protection officer (DPO)

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

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

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

Joy Lane Primary Foundation School has a Data Protection Officer (DPO).
The school's DPO is: https://www.satswana.com/ and can be contacted at: info@satswana.com

The main duties of the DPO are:

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

In addition, the school lead DPO can be contacted through our School Business Manager and via dpo@joylane.kent.sch.uk

Headteacher

The headteacher 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 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

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.

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 pupil) has freely given clear **consent**

For special categories of personal data, we will also meet 1 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.

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

- Joy Lane Primary Foundation School 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 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

Joy Lane Primary Foundation School will also share personal data with law enforcement and government bodies where we are legally required to do so.

Joy Lane Primary Foundation School 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.

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 can be submitted in any form, including verbal and through social media, 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.

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 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 our school may 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.

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.

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 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 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.

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.

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 school Data Protection Officer

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 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 the pupil.

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 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 photographer, newspapers, campaigns
- Online on our school website or social media pages

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

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

See our child protection and safeguarding policy/photography policy/other relevant policy for more information on our use of photographs and videos.

Photographs are also shared via ClassDojo which parents consent to when they sign up. Please see the ClassDojo privacy policy that is agreed when parents sign up and connect to the website / app.

Artificial intelligence (AI)

Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Joy Lane Primary Foundation School recognise that AI has many uses to help pupils 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, Joy Lane Primary Foundation School will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing 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

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.
- No laptops store information on the hard drives, all documents are saved on staff 'one drive' accounts in the cloud and the one drive accounts can only be accessed with passwords.
- 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 8 characters long containing upper- and lower-case letters, numbers and special characters - 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
- Staff are reminded not to use removable devices such as USB drives for any documents containing personal data and to save these documents on their secure 'one drive' accounts. If a removeable device is required, it will be protected with encryption software.
- 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 online 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 (see section 8)

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 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

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.

Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy notices, please see
    - Appendix 2 for Pupils
    - Appendix 3 for Pupils in need and looked After
    - Appendix 3 for Parents
    - Appendix 4 for School Workforce

Appendix 1

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@joylane.kent.sch.uk ad describe in detail the nature of the breach
- 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 on the school computer system
- 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 on the school computer system
- 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 when required 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 External IT support provider to attempt to recall it from external recipients and remove it from the school email system retaining a copy if requires 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 endeavor 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 DSL and discuss whether the school should inform any or all, of its 3 local safeguarding partners.

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 2

Privacy Notice - How we use pupil information

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to support you to decide what to do after you leave the school

Categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility, pupil premium, looked after)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- National curriculum assessment results
- Relevant medical information (such as medical condition, medication, dietary requirements, emergency contact details, parent/carer authorisation)
- Special education needs information
- Pastoral records (such as, consent forms-Photographs/School trips, behavioral incidents, attendance record, accident reports
- Admission record
- Safeguarding information (such as concerns logged, referrals made, disclosure, action taken)
- Academic information (such as formative assessment results, summative assessment results, exam results, in-Class aptitude data, parent reports, records of intervention provided

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupils' information to us or if you have a choice in this.

Storing pupil information

Joy Lane Foundation Primary School keeps information about you on computer systems and also on paper.

We hold your education records securely until you change school. Your records will then be transferred to your new school, where they will be retained until you reach the age of 25, after which they are safely destroyed.

There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it is the only way we can make sure you stay safe and healthy or we are legally required to do so.

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

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

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

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

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational

performance to inform independent research, as well as studies commissioned by the DfE. 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 pupils to the DfE as part of statutory data collections such as school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

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

To find out more about the NPD, please visit:

https://www.gov.uk/government/publications/national-pupil-database-user-guide- and-supporting-information

The department may share information about our pupils 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 pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements, retention, and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/guidance/data-protection-how-we-collect-and-shareresearch-data

For information about organisations the department has provided pupil information, (and for which project), please visit:
https://www.gov.uk/guidance/data-protection-how-we-collect-and-shareresearch-data

Requesting access to your personal data

Under data protection legislation, parents and pupils 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 School Business Manager and/or Data Protection Officer

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 any 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 get a copy of the information about you that KCC shares with the DfE or how they use your information, please contact:

Information Resilience & Transparency Team

Room 2.71, Sessions House, Maidstone, Kent, ME14 1XQ mailto:

dataprotection@kent.gov.uk

You can also visit the KCC website if you need more information about how KCC use and store information, please visit: http://www.kent.gov.uk/about-thecouncil/contact- us/access-to-information/your-personal-information to contact DfE, please visit: https://www.gov.uk/contact-dfe

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

The School Business Manager and /or Data Protection Officer

Name:	Data Protection Officer
Email:	info@staswana.com
Correspondence address:	Data Protection Officer Pembrooke House St Christopher's Place Farnborough, Hampshire. GU14 0NH

Appendix 3

Privacy Notice- **How we use children in need and children looked after information**

Categories of this information that we collect, process, hold and share include:

- Personal information (such as name, date of birth and address)
- Special categories of data including characteristics information (such as gender, age, ethnic group)

- Characteristics (such as gender, ethnicity and disability)
- Information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child protection information and child Protection Plan information)

- Episodes of being looked after (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)

- Adoptions (such as dates of key court orders and decisions)
- Care leavers (such as their activity and what type of accommodation they have)

Why we collect and use this information

We use this data to:

- Support these children and monitor their progress
- Provide them with pastoral care
- Assess the quality of our services
- Evaluate and improve our policies on children's social care

The lawful basis on which we process this information

We collect and process information about children in our care and children to whom we provide services under

- Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- Article 9(2)(b) processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security agreement pursuant to member state law providing for the appropriate safeguards for the fundamental rights and the interests of the data subject.

The Education Act 1996; this information can be found in the guide documents on the following website: https://www.gov.uk/education/data-collection-andcensuses- for-schools

Collecting this information

Whilst the majority of children looked after information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, 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

Joy Lane Foundation Primary School keep information about children in need and children looked after on computer systems and also some on paper.

We hold your education records securely until you change school. Your records will then be transferred to your new school, where they will be retained until you reach the age of 25, after which they are safely destroyed.

There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it is the only way we can make sure you stay safe and healthy or we are legally required to do so.

Who do we share this information with?
We routinely share pupil information with:

- the Department for Education (DfE)

Why we share this information

Department for Education (DfE)- We share children in need and children looked after data with the Department for Education (DfE) on a statutory basis under section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information about Individual Pupils) (England) Regulations 2013.

This data sharing help to develop national policies, manage local authority performance, administer and allocate funding and identify and encourage good practice.

We do not share information about our children in need or children looked after with anyone without consent unless the law and our policies allow us to do so.

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education please visit:

Children looked after:

https://www.gov.uk/guidance/children-looked-after-return-guide-to-submitting-data

Children in need: https://www.gov.uk/guidance/children-in-need-census

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. 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 pupils to the DfE as part of statutory data collections such as school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, please visit:

https://www.gov.uk/government/publications/national-pupil-database-user-guide- and-supporting-information

The department may share information about our 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 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 school workforce information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements, retention, and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/guidance/data-protection-how-we-collect-and-shareresearch-data

For information about organisations the department has provided pupil information, (and for which project), please visit:
https://www.gov.uk/guidance/data-protection-how-we-collect-and-shareresearch-data

To contact the Department for Education, please visit: 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, please contact:

The School Business Manager and/or Data Protection Officer

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 any 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/ **Further Information** if you would like to discuss anything in this privacy notice, please contact:

The School Business Manager and /or Data Protection Officer

Name: Data Protection Officer

Email: info@satswana.com

Correspondence address: Data Protection Officer

Pembrooke House

St Christopher's Place Farnborough,
Hampshire.
GU14 0NH

Appendix 4

Privacy Notice

How we use school workforce information

Categories of school workforce information that we collect, process, hold and share include:

- Personal information (such as name, address, contact information, employee or teacher number, national insurance number)
- Special categories of data including characteristics information (such as gender, age, ethnic group)
- Contract information (such as start dates, hours worked, post, roles and payroll information, promotion information)
- Attendance information (such as number of absence and reasons)
- Qualifications
- Training information
- Medical information if applicable
- Performance management information (such as Appraisals, grievances
- Disciplinary / capability procedures if applicable
- Vehicle registration if applicable
- Accident at work

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

- Performance management
- Training records
- Monitor attendance

The lawful basis on which we process this information

We process this information under

- Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Article 9(2)(b) processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security agreement pursuant to member state law providing for the appropriate safeguards for the fundamental rights and the interests of the data subject.

The Education Act 1996; this information can be found in the guide documents on the following website: https://www.gov.uk/education/data-collection-and-censusesfor-schools

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 the General Data Protection Regulation, 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 for the retention periods stated in the Information Management Toolkit for school.

There are strict controls on who can see your information. We will not share your data if you have advised us that you do not want it shared unless it is the only way we can make sure you stay safe and healthy or we are legally required to do so.

Who do we share this information with?

We routinely share pupil information with:

- our local authority
- the Department for Education (DfE)
- our Payroll and Personnel providers

Why we share school workforce information

We do not share information about our pupils 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 (DfE0 on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment 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.

Payroll and Personnel Providers

We share personal information to inform contractual / personal changes, overtime and absence information.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupils 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 Department for Education including the data that we share with them, please visit:
https://www.gov.uk/education/data-collection-and-censuses-for-schools

The department may share information about our 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 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 school workforce information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements, retention, and use of the data.

For more information about the department's data sharing process, please visit:

https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

To contact the Department, please visit: 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, please contact:

the Data Protection Officer,

Contact: dpo@joylane.kent.sch.uk

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 any 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/ **Further Information** if you would like to discuss anything in this privacy notice, please contact:

The School Business Manager or the Data Protection Officer

Name: Data Protection Officer

Email: info@satswana.com

Pembrooke House

St Christopher's Place

Farnborough, Hampshire. GU14 0NH