SESSET

Privacy Notice – Pupils

REVIEWED AND APPROVED BY TRUSTEES ON:	
NEXT REVIEW DATE:	**Summer term 2027**

Carrington School, Therfield School and The Ashcombe School have formed and are part of South East Surrey Schools Education Trust (SESSET), a charitable company limited by guarantee and registered in England and Wales with company number 10479401. The registered address is The Ashcombe School, Ashcombe Road, Dorking, Surrey RH4 1LY

Privacy Notice (How we use pupil information)

South East Surrey Schools Education Trust (SESSET) is the data controller for the pupil information described in this notice. This means we decide how and why it is used. SESSET is registered on the data protection register (registration number ZA228701).

This notice explains how Carrington School, Therfield School and The Ashcombe School use information about their pupils, and about pupils' parents and carers. It is written for parents and carers and for older pupils. We will explain it to younger pupils in a way they can understand.

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

- Personal information (such as name, date of birth, address, unique pupil number, unique learner number and photograph)
- Information for parents, guardians, carers, those with responsibility, and/or key adults (such as names, addresses, contact numbers, and emails)
- 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)
- Assessment and attainment information (such as test and exam results, and work pupils produce in class and online)
- Medical and health information (such as doctors' details, allergies, medication and dietary requirements)
- Special educational needs information
- Behaviour information (such as suspensions, exclusions and any alternative provision)
- Post 16 learning information
- Safeguarding information (such as court orders and the involvement of other professionals)
- Information about how pupils use our IT systems and online learning platforms, including sign-in records and internet filtering and monitoring records
- Photographs, video and CCTV images
- Biometric information, where a school uses fingerprint recognition (for example to pay for school meals) and consent has been given

Why do we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- for communication relating to a pupil's education and care
- to provide appropriate pastoral care

- to keep pupils safe, including safeguarding, managing allergies and medical needs, and contacting parents and carers in an emergency
- to assess the quality of our services
- to comply with the law regarding data sharing
- to support pupils in their next steps (e.g. references)
- to give pupils access to Microsoft 365, Teams and the educational apps we use to support learning, including homework
- to keep our IT systems secure and help keep pupils safe online, through internet filtering and monitoring
- to meet the statutory duties placed on us for Department for Education data collections
- to respond to requests people make to see the information we hold about them

The lawful basis on which we use this information

We use pupil information under Article 6 of the UK GDPR because it is necessary to carry out a task in the public interest, which is educating pupils and running our schools (Article 6(1)(e)), and because we have to comply with legal obligations, such as the school census and attendance registers (Article 6(1)(c)).

Sometimes we seek consent (Article 6(1)(a)) to use a pupil's photograph in publicity, to provide an optional app or service, or for biometric recognition. Consent can be withdrawn at any time by contacting the school. In an emergency, we may share information to protect a pupil's vital interests (Article 6(1)(d)).

When we process special category information, such as health, ethnicity, special educational needs, or biometric information, we also rely on a condition in Article 9 of the UK GDPR. This is usually substantial public interest (Article 9(2)(g)), with the relevant condition in Schedule 1 to the Data Protection Act 2018, such as safeguarding children or equality of opportunity. We rely on explicit consent (Article 9(2)(a)) for biometric information, and on vital interests (Article 9(2)(c)) in an emergency. Any information about criminal offences, for example where the police are involved, is processed under Article 10 and Schedule 1 of the Data Protection Act 2018.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some is provided voluntarily. To comply with data protection legislation (the UK GDPR and the Data Protection Act 2018), we will inform you whether you are required to provide certain pupil information to us or whether you have a choice.

We also receive information about pupils from their previous school, the local authority and the Department for Education, for example through the Common Transfer File.

Storing pupil data

We retain pupil information for as long as set out in the SESSET Data Retention Policy, and then securely delete it. When a pupil moves to another school, their educational

record accompanies them. We hold information about children in need and children looked after in line with the Department for Education's guidance.

Educational apps and online services

Our schools use a range of educational apps and websites to support pupils' learning, for example for reading, maths, languages, revision and homework. Before we introduce an app, we check that it is needed and that it protects pupils' information. Where the risk is higher, we complete a data protection impact assessment. We only use apps that:

- act on our instructions as our data processor, under a contract
- receive only the information needed, usually the pupil's name, class and school email address, often through a Microsoft sign-in

We use only artificial intelligence (AI) tools approved by the school. Pupils' personal information is not entered into public AI tools, and approved tools must not use pupils' information or work to train their AI models.

Photographs, CCTV and biometric information

We use photographs for identification, for example in Arbor and CPOMS. We seek consent before using a pupil's photograph or video in publicity, such as on our websites or social media. We use CCTV to keep our sites safe and secure.

Where a school uses fingerprint recognition, we will obtain written consent from a parent or carer first, as required by the Protection of Freedoms Act 2012. A pupil can refuse to take part at any time, even if a parent has consented, and an alternative will always be provided. Further details are available in the SESSET Protection of Biometric Information Policy.

Systems we use to hold pupil information

The systems below hold most of the personal information we keep. Each supplier is our data processor. This means it may use the information only on our written instructions, under a contract that meets Article 28 of the UK GDPR, and must keep the information secure and confidential, deleting it when our contract ends. None of these suppliers may sell the information, use it for advertising, or use it to train their own artificial intelligence models. We carry out a data protection impact assessment before introducing a system like these and review it when circumstances change.

Microsoft 365

- **Supplier:** Microsoft.
- **What we use it for:** pupils' school accounts and email; storing and sharing work in OneDrive, SharePoint and OneNote class notebooks; quizzes and forms; and signing in to the educational apps we use.

- **Information held:** name, school email address, year and class groups, work pupils create and save, emails, and sign-in and activity records that we use to keep accounts secure and help keep pupils safe online.
- **Where it is stored:** Microsoft stores our data in its UK data centres. See 'Transferring information outside the UK' below.
- **Safeguards:** Microsoft's Data Protection Addendum, which makes Microsoft our processor; access limited to people who need it; multi-factor authentication for staff; and security monitoring.
- **How long:** pupils' accounts, and the work and emails in them, are deleted after a pupil leaves, in line with the SESSET Data Retention Policy.

Microsoft Teams

- **Supplier:** Microsoft. Teams is part of Microsoft 365, with the same safeguards and UK storage.
- **What we use it for:** class teams, sharing learning resources, homework via Teams Assignments (including feedback and marks), messages between staff and pupils, and online lessons and meetings. The Ashcombe School also uses Teams to send a homework update email to parents.
- **Information held:** name, class memberships, posts and messages, work handed in, feedback and marks and, if a meeting is recorded or transcribed, the recording or transcript, parental email addresses for homework updates.
- **How long:** in line with the SESSET Data Retention Policy.

Arbor

- **Supplier:** Arbor Education Partners Limited.
- **What we use it for:** our management information system: registers and attendance, behaviour and achievement, assessment and reports, timetables, exam entries, SEN and medical information, and communication with parents and carers, including through the Arbor app. We also use it to produce the school census for the Department for Education.
- **Information held:** pupils' and parents' and carers' contact details, photographs, and the other categories of information listed at the start of this notice.
- **Where it is stored:** Arbor stores and backs up all data in the UK, in Amazon Web Services' London data centre.
- **Safeguards:** access is role-based, so staff only see what they need for their job.
- **How long:** in line with the SESSET Data Retention Policy. When a pupil changes school, we send their record to the new school via the Common Transfer File.

CPOMS

- **Supplier:** CPOMS Systems Limited.

- **What we use it for:** recording and managing safeguarding and wellbeing concerns about pupils, and the action we take.
- **Information held:** concerns and incidents, actions taken, contact with other agencies such as children's services and the police, and supporting documents. This can include health information, family circumstances and other sensitive information.
- **Who can see it:** access is restricted by role. Only designated safeguarding leads and other staff who need it can see full records, and all access is logged.
- **Where it is stored:** CPOMS stores data in the UK.
- **Safeguards:** data is encrypted when stored and when sent, and access requires multi-factor authentication.
- **How long:** safeguarding records are kept in line with Keeping Children Safe in Education and the SESSET Data Retention Policy. When a pupil moves schools, we transfer their safeguarding file securely to the new school.

Fisar

- **Supplier:** Fisar UK Ltd (company number 16926890).
- **What we use it for:** to help us respond to subject access requests, which are requests from people for a copy of the information we hold about them.
- **How it works:** when someone makes a subject access request, Fisar searches our Microsoft 365 systems (including email, OneDrive, SharePoint and Teams chats), Arbor and CPOMS, on a read-only basis, to find information about that person. It uses automated tools, including artificial intelligence, to find information about other people so that it can be redacted (blacked out). A member of our data protection team checks the identity of the person making the request and reviews every document and every redaction before anything is released. Fisar does not make decisions about anyone.
- **Whose information:** the person making the request, and anyone else mentioned in the records found, such as pupils, parents and staff. Other people's information is only released where the law allows.
- **Where it is stored:** Fisar keeps data in Amazon Web Services' London data centre and does not process it outside the UK or the European Economic Area.
- **Safeguards:** Fisar only has read access to our systems, data is encrypted, access requires multi-factor authentication, and each school's data is kept separately.
- **How long:** working copies are deleted within 30 days of a request being closed. Fisar keeps an audit record of the steps taken on each request for seven years, and we keep our own record of each request in line with the SESSET Data Retention Policy.
- **Lawful basis:** responding to subject access requests is a legal obligation under Article 15 of the UK GDPR (Article 6(1)(c)). Where the records found include special category information, we rely on the conditions already described in this notice.

Transferring information outside the UK

We store information in the UK wherever possible. Arbor keeps data in the UK, Fisar keeps data in the UK or the European Economic Area (which is covered by UK adequacy regulations), and Microsoft stores our Microsoft 365 data in its UK data centres. Some suppliers, such as Microsoft, may access or process limited information outside the UK, for example to provide technical support or security services. Where this happens, we make sure the information is protected to UK standards: for example, because the country is covered by UK adequacy regulations (including the UK–US data bridge for certified US companies), or because the supplier has agreed to the UK International Data Transfer Agreement or Addendum.

Who we share pupil information with

We routinely share pupil information with:

- schools and colleges that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- Support services such as CAMHS
- Medical and Emergency services
- exam boards and awarding bodies, to enter pupils for exams and apply for access arrangements
- the Learning Records Service (part of the DfE), for pupils aged 14 and over
- the NHS school nursing and immunisation service
- Surrey County Council children's services, the police and other agencies, where needed to keep a child safe
- our data processors: Microsoft, Arbor, CPOMS, Fisar and the providers of our educational apps

Why do we share pupil information

We share pupil information only where the law permits, and we never sell it. We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding, educational attainment policy, and monitoring. We are required to share information about our pupils with the DfE under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

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

Learning Records Service

For pupils aged 14 and over, we give the Learning Records Service the pupil's name, date of birth, and gender so it can issue a unique learner number and add qualifications to the pupil's personal learning record. To find out more, go to

https://www.gov.uk/government/publications/privacy-information-key-stage-4-and-5-and-adult-education.

Youth support services

Pupils aged 13+
Once our pupils reach the age of 13, we also pass pupil information to our local authority and/or the provider of youth support services, as they have responsibilities for 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 or guardian can request that only their child's name, address and date of birth be passed to their local authority or provider of youth support services by informing us. This right transfers to the child/pupil once they reach the age of 16.

Pupils aged 16+
We will also share certain information about pupils aged 16+ with our local authority and/or the provider of youth support services, as they have responsibilities for the education or training of 13-19-year-olds under section 507B of the Education Act 1996.

This enables them to provide the following services:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information on pupils in schools in England. It provides invaluable evidence on educational performance to inform both independent research and studies commissioned by the Department. It is held electronically 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 the school census and the early years' census. Some of this information is stored in the NPD. The law that permits this is the Education (Information About Individual Pupils) (England) Regulations 2013.
To find out more about the NPD, go to 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 children's education or well-being 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 over access to and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and are 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, and the 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 on which organisations the department has provided pupil information to, and for which project, please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received.

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

Requesting access to your personal data

Under data protection legislation, pupils have the right to request a copy of the information we hold about them. Parents and carers can make a request on their child's behalf. Once a pupil is around 12 or older and able to understand their rights, we will usually consider whether they have agreed. We will respond within one month, carrying out reasonable and proportionate searches. If we need more information to locate the requested information, we will ask, and the time limit will pause until we receive it. To make a request or to access your child's educational record, contact:

- Mr James Robinson – SESSET Data Protection Officer, robinson.james@ashcombe.surrey.sch.uk, or at The Ashcombe School, Ashcombe Road, Dorking RH4 1LY.
- Mr Matt Houghton – Data Protection Lead, mhoughton@therfield.surrey.sch.uk, or at Therfield School, Dilston Road, Leatherhead, SURREY, KT22 7NZ.
- Mr Ben Stafford - Data Protection Lead, bstafford@carringtonschool.org, or at Noke Drive, Redhill, RH1 4AD.

We use Fisar to help us find and prepare the information for a subject access request, as described in 'Systems we use to hold pupil information'.

You also have the right to:

- be told how we use your information, which this notice does
- have inaccurate information corrected
- ask us to delete information or restrict how we use it, in certain circumstances
- withdraw consent at any time, where we rely on consent
- ask for information to be transferred to another organisation, in certain circumstances

We do not make decisions about pupils using solely automated processing.

If you have a concern about how we collect or use your personal data, you have the right to complain to us, either electronically (for example, by emailing the DPO) or by post. We will acknowledge your complaint within 30 days and respond without undue delay (section 164A of the Data Protection Act 2018). If you are not satisfied with our response, you can complain to the Information Commission (which continues to operate as the ICO) under section 165 of the Data Protection Act 2018 at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please get in touch with us:

- Mr James Robinson – SESSET Data Protection Officer, robinson.james@ashcombe.surrey.sch.uk, or at The Ashcombe School, Ashcombe Road, Dorking, Surrey, RH4 1LY.

Appendix 1

Privacy Notice (How we use children in need and children looked after information)

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

- personal information (such as name, date of birth and address)
- characteristics (such as gender, ethnicity and disability)
- information relating to episodes of being a child in need (such as referral, assessment, Section 47, Initial Child Protection and Child Protection Plan information)
- episodes of being looked after (such as important dates and information on placements)
- outcomes for looked-after children (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 activities and the type of accommodation they have)
- relevant medical information
- special educational needs information
- behavioural information

Why do we collect and use this information

We use this personal 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 use this information: We process this information to comply with our legal obligations and to perform a task carried out in the public interest (Article 6(1)(c) and (e) of the UK GDPR). For special category data, we rely on Article 9(2)(b) and (g) of the UK GDPR, together with the relevant conditions in Schedule 1 to the Data Protection Act 2018, and in connection with our duties under the Children Act 1989 and the Children Act 2004.