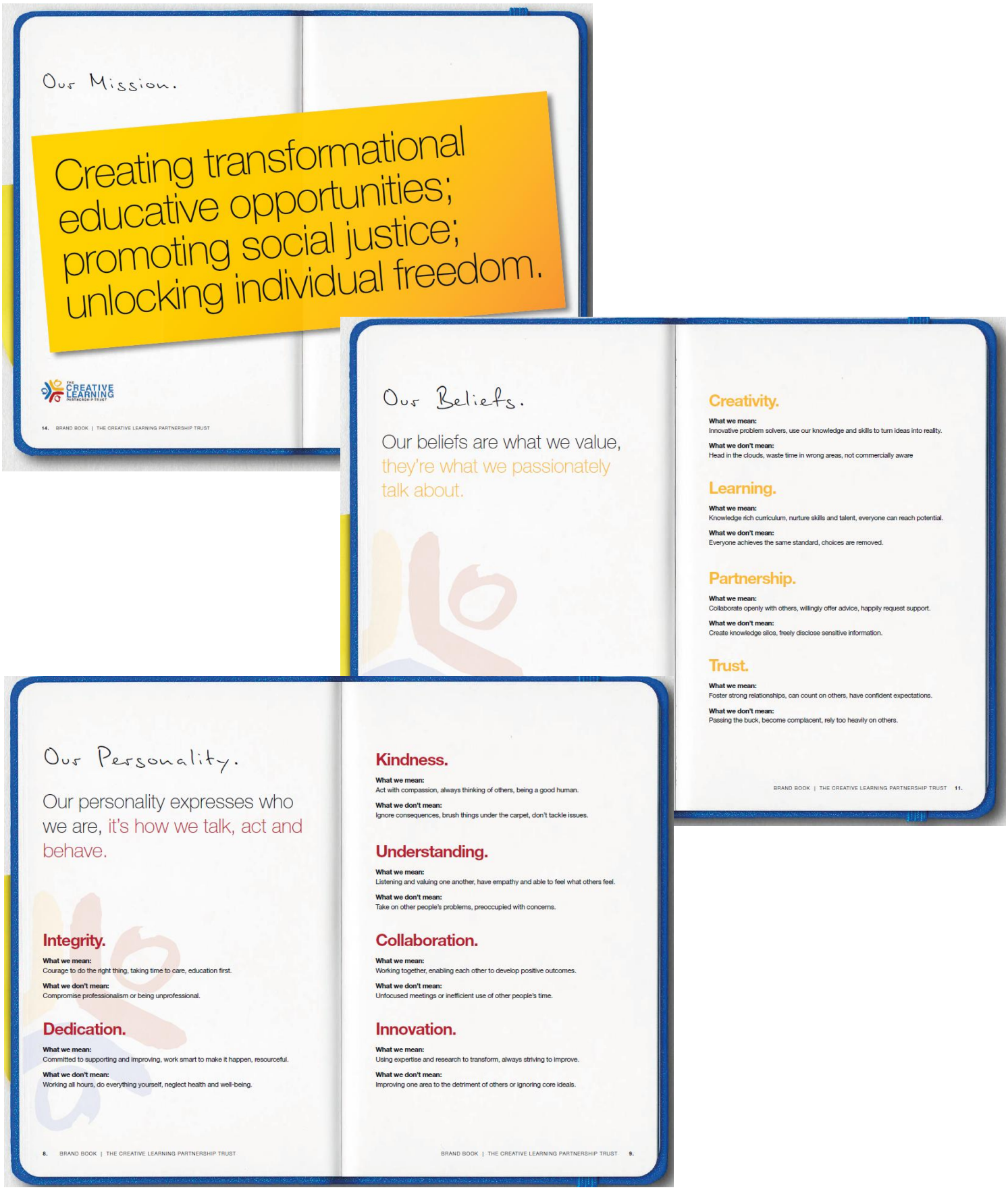
THE CREATIVE LEARNING PARTNERSHIP TRUST

Privacy Notice for Pupils, Parents & Carers

Responsible Committee	CLPT Finance and Operations Committee
Date Approved by Committee	9th December 2025
Implementation Date	9th December 2025
Next Review Date	Autumn Term 2026
Policy Owner	Laura Austen

This Policy has been created in accordance and to support the Mission, Values and Beliefs of The Creative Learning Partnership Trust.



This privacy notice applies to all schools within The Creative Learning Partnership Trust:

- **Hempstalls Primary School**
- **James Bateman Middle School**
- **Langdale Primary School**
- **Manor Hill First School**
- **Parkside Primary School**
- **Thursfield Primary School**
- **Greenhall School**
- **Green Lea First School**
- **Beaconfields Primary School**
- **Doxey Academy**
- **Burleyfields Primary School**

Under data protection law, individuals have a right to be informed about how the Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, The Creative Learning Partnership Trust, c/o Beaconfields Primary School, Ramson Avenue, Stafford, Staffs, ST16 1ZY, are the 'data controller' for the purposes of data protection law.

Our data protection officer is
Hedda Motherwell , Staffordshire County Council (see '*Contact Us*' below)

Quick Reference: What Systems Hold My Child's Data?

Type of Information	**Main Systems Used**
Core pupil records (attendance, assessment, contact details)	Arbor MIS
Safeguarding records	MyConcern
Online learning and homework	Microsoft 365 (Teams), Spelling Shed, Times Table Rockstars
School payments	ParentPay
Email and documents	Microsoft 365
Internet safety monitoring	Securus
Website information (with consent)	Juniper Websites

For a full list of systems and detailed information about what data they hold, see the "Digital Systems and Third-Party Platforms We Use" section below.

The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents, parental responsibility information, national insurance numbers as and when required
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information

- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information / Child Protection information
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school/ on school premises
- Court orders / legal documents

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Photographs, Videos and CCTV

We may take photographs and videos of pupils for various purposes, including:

- Displays within the school
- The school website and prospectus
- Social media (school accounts only)
- Local and national media coverage
- Educational purposes and recording achievements

We will seek your consent before using photographs or videos of your child, and you can withdraw consent at any time. Different types of use may require separate consent (for example, we may ask separately for consent to use images on social media).

We will not use images of pupils if:

- You have withdrawn consent
- There are safeguarding concerns that make it inappropriate
- The child has asked us not to

CCTV

We use CCTV systems in and around our school premises for the safety and security of pupils, staff and property. CCTV footage is typically retained for 30 days unless required for investigation or legal proceedings.

Parents and carers taking photographs

We ask parents and carers to be mindful when taking photographs or videos at school events. Please:

- Only take photos/videos of your own child where possible
- Do not share images of other children on social media without their parents' consent
- Follow any specific guidance provided by the school for individual events

---

Information We Hold About Parents and Carers

We also collect and hold personal information about parents and carers, including:

- Names and contact details (address, phone numbers, email addresses)
- Relationship to the child and parental responsibility information
- Communication preferences
- Employment information (for free school meals eligibility assessments)

- Financial information (for dinner money, school trips, and other payments)
- Records of communications with the school
- ParentPay/Arbor account information
- Attendance at school events

We use this information to:

- Communicate with you about your child's education and wellbeing
- Ensure we contact the right people in an emergency
- Process payments for school services
- Comply with our legal obligations
- Assess eligibility for support (such as free school meals or pupil premium funding)

The same rights outlined in this privacy notice apply to your personal data as well as your child's.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Special Category Data

Some of the personal information we collect is classified as 'special category data' under data protection law. This includes information about:

- Racial or ethnic origin
- Religious beliefs
- Health data (including physical and mental health, medical conditions, dietary requirements)
- Biometric data (where used for identification purposes)

We process special category data in accordance with the Equality Act 2010 and data protection law. We only process this data where we have a lawful basis to do so, which includes:

- Where it is necessary for reasons of substantial public interest (such as safeguarding children or meeting our statutory duties)
- Where you have given explicit consent
- Where it is necessary to protect the vital interests of the pupil or another person
- Where it is necessary for the provision of health or social care

We take extra care to protect special category data and ensure it is only accessed by staff who need it to carry out their roles.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

How long we keep this data

We keep personal information about pupils in accordance with legal requirements and our data retention schedule. Below are the typical retention periods for different types of information:

Type of Information	Retention Period
Pupil files (including academic records)	**Until the pupil reaches 25 years of age**
Child protection and safeguarding records	**Until the pupil reaches 25 years of age (or longer if required by safeguarding circumstances)**
Special educational needs (SEND) files	**Until the pupil reaches 25 years of age**
Accident and injury records	**Until the pupil reaches 25 years of age**
Attendance registers	**3 years from the date of the last entry**
Admission registers	**3 years from the date of the last entry**

Type of Information	Retention Period
Exclusion records	**Until the pupil reaches 25 years of age**
CCTV footage	**Typically 30 days, unless required for investigation or legal proceedings**
Photographs and videos (with consent)	**While the pupil attends the school, unless consent is withdrawn**

Where children leave the school, the designated safeguarding lead will ensure their child protection file is transferred to the new school or college as soon as possible, and within 5 days for an in-year transfer or within the first 5 days of the start of a new term.

We may retain information for longer than the periods stated above where we have a legal obligation to do so, or where it is necessary for the establishment, exercise or defence of legal claims.

When Your Child Leaves Our Schools

When your child leaves one of our schools, we will transfer their educational records and child protection file to their new school or educational setting securely and within the required timeframes.

We will continue to hold some information about former pupils in accordance with our retention schedule (see "How long we keep this data" above).

We do not currently maintain an alumni database. If we decide to do so in the future, we will contact former pupils and their families to seek consent and explain how the information will be used.

Former pupils have the same rights as current pupils to request access to their information, request corrections, or ask for their data to be erased (subject to our legal obligations to retain certain records).

Data sharing

We may share personal information with third party providers in support of our teaching and learning function and where the law and our policies allow us to do so. Consent will be sought where it is necessary.

Where it is legally required or necessary (and it complies with data protection law) we may share personal information about pupils with:

- *Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions, information for 2 and 3 year old funding*
- *The Department for Education – census information*
- *The pupil's family and representatives – only with parents or representatives with parental responsibility unless parents have specified otherwise.*
- *Educators and examining bodies – to meet our legal obligations*
- *Our regulator - Ofsted*
- *Suppliers and service providers – to enable them to provide the service we have contracted them for*

- *Financial organisations – Parentpay/Arbor*
- *Central and local government – to meet legal obligations in respect of statutory returns*
- *Our auditors – to meet the legal obligations of a multi academy trust*
- *Survey and research organisations*
- *Health authorities*
- *Security organisations*
- *Health and social welfare organisations*
- *Professional advisers and consultants*
- *Charities and voluntary organisations – where we have sought parental consent for them to work with your child*
- *Police forces, courts, tribunals*

Safeguarding and Child Protection

Safeguarding and promoting the welfare of children is everyone's responsibility. Information sharing is vital in identifying and tackling all forms of abuse, neglect, and exploitation.

We may share personal information without consent where there is good reason to do so, and where the sharing of information will enhance the safeguarding of a child in a timely manner. It would be legitimate to share information without consent where: it is not possible to gain consent; it cannot be reasonably expected that we gain consent; and, if to gain consent would place a child at risk.

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe.

We may share safeguarding information with:

- Local authority children's social care
- The police
- Health services
- Other schools (when a child transfers)
- Multi-agency safeguarding partners

Our approach to safeguarding is set out in our Child Protection and Safeguarding Policy, which is available on our school websites.

School Trips and Educational Visits

When your child participates in school trips or educational visits, we may need to share personal information with:

- Trip organisers and activity providers
- Transport companies
- Accommodation providers
- Medical services (in case of emergency)

The information we share typically includes:

- Your child's name and date of birth
- Emergency contact details
- Medical information and dietary requirements
- Any special educational needs or accessibility requirements

We only share the minimum information necessary to ensure your child's safety and wellbeing during the trip. All third parties are required to handle this information in accordance with data protection law.

Digital Systems and Third-Party Platforms We Use

To support teaching, learning, school administration and communication, we use various digital systems and platforms. Below is a list of the main systems we use across The Creative Learning Partnership Trust, what they're used for, and what type of data they process.

Core School Systems

Microsoft 365 (https://www.microsoft.com/en-gb/privacy/privacystatement)

- Purpose: Email, document creation and storage, online learning (Teams), video conferencing
- Data processed: Staff and pupil names, email addresses, documents created, communication records
- Location of data: UK and European data centres with appropriate safeguards

Arbor Management Information System (MIS) (https://support.arbor-education.com/hc/en-us/article_attachments/21374019354269)

- Purpose: Central database for pupil records, attendance, assessment, timetabling, reporting, admissions
- Data processed: Pupil personal details, contact information, attendance records, assessment data, medical information, SEND information, behaviour records, safeguarding information
- Location of data: UK data centres
- Note: Arbor is our primary school management system and holds the most comprehensive pupil data

Windows Active Directory (AD)

- Purpose: Network access management and security
- Data processed: User accounts, login credentials, access permissions
- Location of data: On school premises and secure cloud backup

Communication and Payment Systems

ParentPay (https://www.parentpay.com/privacy-notice/)

- Purpose: Cashless payment system for school meals, trips, and other school services
- Data processed: Parent/carer names, contact details, payment information, pupil meal preferences
- Location of data: UK data centres
- Note: ParentPay is PCI-DSS compliant for secure payment processing

Universe VoIP (https://firstcomeurope.co.uk/wp-content/uploads/2025/10/P20-Privacy-Policy-02.23.pdf)

- Purpose: School telephone system
- Data processed: Call records, voicemail messages
- Location of data: UK data centres

Governor Hub (https://help.governorhub.com/en/articles/586895-privacy-policy)

- Purpose: Governance management and document storage

- Data processed: Governor details, meeting minutes, governance documents (may include references to pupils in safeguarding or exclusion matters)
- Location of data: UK data centres

Website and Communication

Juniper Websites (https://websites.junipereducation.org/privacy-cookies/)

- Purpose: School websites
- Data processed: Information published on school websites (may include pupil photographs with consent, staff information, school policies)
- Location of data: UK hosting

Learning and Assessment Platforms

Spelling Shed (https://www.edshed.com/en-gb/privacy)

- Purpose: Online spelling practice and assessment
- Data processed: Pupil names, class information, spelling assessment results, login credentials
- Location of data: UK data centres

Times Table Rockstars (https://mathscircle.com/privacy-notice)

- Purpose: Online times tables practice and assessment
- Data processed: Pupil names, class information, mathematics assessment results, login credentials
- Location of data: UK data centres

Safeguarding and Wellbeing Systems

MyConcern (https://www.tes.com/en-gb/policies/privacy-notice)

- Purpose: Safeguarding and child protection record-keeping
- Data processed: Safeguarding concerns, child protection records, incident reports, staff actions taken
- Location of data: UK data centres
- Note: This system holds highly sensitive special category data and is subject to strict access controls

Securus (https://www.securus-software.com/legal/privacy-policy/)

- Purpose: Online safety monitoring (monitoring of school network activity)
- Data processed: Internet usage logs, flagged concerning online activity
- Location of data: UK data centres
- Note: Used to keep pupils safe online in accordance with our Online Safety Policy

Data Management and Security Systems

Wonde (https://www.wonde.com/privacy-policy/)

- Purpose: Secure data sharing between our MIS (Arbor) and other educational platforms. Wonde processes and collects data to facilitate data integration, enhance school management, support teaching and learning, ensure data security, and comply with data protection regulations.
- Data processed: Acts as a data 'bridge' - transfers pupil and staff data between systems as authorised
- Location of data: UK and EU data centres with appropriate safeguards

Redstor https://www.redstor.com/privacy-policy/

- Purpose: Backup and disaster recovery
- Data processed: Backup copies of all school data
- Location of data: UK data centres with encryption

Barracuda https://trust.barracuda.com/privacy/documentation/privacy-notice

- Purpose: Email security and filtering
- Data processed: Email content and metadata for security scanning
- Location of data: UK and EU data centres

DCPro (Data Collection Pro) https://www.dcpro.co.uk/privacy-policy-2/

- Purpose: Data collection for statutory returns (school census, etc.)
- Data processed: Pupil and staff data required for DfE census returns
- Location of data: UK data centres

How We Ensure These Systems Are Safe

When we use third-party systems and platforms, we:

✓ Conduct due diligence before selecting any system to ensure the provider has appropriate data protection measures in place

✓ Have data processing agreements in place with all providers, which set out their responsibilities under UK data protection law

✓ Only share the minimum data necessary for each system to function

✓ Ensure appropriate security measures are in place, including encryption, secure access controls, and regular security updates

✓ Check that providers comply with UK GDPR and have appropriate safeguards for any data stored outside the UK

✓ Regularly review our systems to ensure they continue to meet our data protection standards

✓ Provide training to staff on how to use systems safely and in compliance with data protection law

✓ Monitor access to ensure only authorised staff can access pupil data

---

Your Rights Regarding These Systems

You have the right to:

- Know which systems hold information about you or your child
- Request access to the data held in these systems (subject access request)
- Request corrections to inaccurate data
- Object to processing in certain circumstances
- Request deletion of data (subject to our legal retention obligations)

To exercise any of these rights, or if you have questions about how a specific system uses your data, please contact your child's school office or our Data Protection Officer (contact details at the end of this notice).

Changes to the Systems We Use

We may add, remove or change the systems we use from time to time. When we introduce a new system that processes personal data, we will:

- Conduct a data protection impact assessment if necessary
- Ensure appropriate safeguards are in place
- Update this privacy notice
- Inform you if the change significantly affects how we process your data

---

Online Safety and Internet Monitoring

To keep pupils safe online, we monitor internet usage on school devices and networks using Securus. This system:

- Monitors websites visited and searches made on school devices
- Flags concerning content or behaviour (such as searches related to self-harm, radicalisation, or inappropriate content)
- Creates alerts that are reviewed by designated safeguarding staff
- Keeps logs of internet activity

Why we do this:

We have a statutory duty under Keeping Children Safe in Education to ensure pupils are safe online. Monitoring helps us identify pupils who may be at risk and intervene early to provide support.

What happens if concerning activity is detected:

If the system flags concerning activity, our designated safeguarding lead (DSL) or deputy DSL will:

- Review the alert
- Assess whether there is a safeguarding concern
- Take appropriate action, which may include speaking to the pupil, contacting parents/carers, or making a referral to external agencies

Your child's privacy:

While we monitor internet usage for safety purposes, we:

- Only review flagged activity or conduct searches when there is a specific concern
- Do not routinely monitor every website visited by every pupil
- Ensure monitoring is proportionate and necessary for safeguarding
- Keep monitoring logs secure and only accessible to authorised safeguarding staff

This monitoring is carried out under our lawful basis of protecting vital interests and performing a task in the public interest (safeguarding children).

For more information, please see our Online Safety Policy, available on our school websites.

International Data Transfers

Some of the systems we use may store or process data outside the United Kingdom. Where we transfer personal data outside the UK, we ensure that:

- The country has been deemed to provide an adequate level of data protection by the UK government, OR
- We have put in place appropriate safeguards, such as:
    - Standard contractual clauses approved by the UK government

- Binding corporate rules
- The provider's certification under an approved framework

The main systems that may involve international data transfers are:

- Microsoft 365: Data is primarily stored in UK/EU data centres, but Microsoft may access data from other locations for support purposes under strict contractual controls
- Wonde: May use EU data centres with appropriate safeguards in place

All our providers are required to comply with UK data protection law regardless of where data is stored or processed.

If you would like more specific information about where data is stored for any particular system, please contact our Data Protection Officer.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

How We Keep Your Information Safe

We take the security of personal data seriously and have appropriate measures in place to protect it, including:

- Secure IT systems with password protection and encryption
- Regular staff training on data protection and information security
- Controlled access to personal information (staff only access what they need for their role)
- Secure storage of paper records
- Regular backups of electronic data
- Clear procedures for reporting and managing data protection concerns

Data Breaches

Despite our security measures, if a data breach occurs that is likely to result in a risk to your rights and freedoms, we will notify you without undue delay. We will also report serious breaches to the Information Commissioner's Office within 72 hours of becoming aware of them.

If you believe there has been a data breach, please contact our Data Protection Officer immediately.

Automated Decision-Making and Profiling

We do not use automated decision-making or profiling in relation to pupils' or parents' personal data. This means that no decisions that significantly affect your child are made solely by automated systems without human involvement.

If this changes in the future, we will update this privacy notice and inform you of your rights in relation to automated decision-making.

Your information rights

You have the following rights in relation to your personal data:

The right of access

Individuals have a right to make a **'subject access request'** to gain access to personal information that the Trust holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the Trust holds about them.

We have to provide a copy of your information to you free of charge, within 1 month. We can extend the deadline if your request is complex. We have to let you know if the deadline is to be extended within 1 month if this is the case.

Information is provided free of charge unless you request further copies of information we have already provided to you. However, we are permitted to charge a reasonable fee or refuse your request if it is manifestly unfounded or excessive. Any fee will be based on the administrative cost of providing the information to you.

The right of rectification

If you feel that any data that we hold about you is factually inaccurate, you have the right to ask us to correct or rectify it. In order for us to review your request you must provide evidence of the alleged inaccuracy.

The right of erasure

You have a right to ask us to erase information about you. This right will only apply where:

- The personal data is no longer necessary for the purpose which we originally collected it for
- We are relying on consent as the lawful basis for holding the data and you withdraw that consent
- We are processing the data for direct marketing purposes and you object to that processing

Most of the processing carried out by the Trust is governed by legislation, which usually includes how long we have to keep your information for. The right of erasure won't apply where we have a lawful reason to process your data.

The right to erasure also does not apply to information which is being processed in accordance with a 'public task'. This means where we are carrying out a specific task in the public interest, which is laid down by law or exercising official authority. This includes, for example, information being processed for Educational, Health and Social Care purposes.

Your right of rectification and erasure extends to anyone we have disclosed your personal information to. We will take reasonable steps, where it is practicable for us to do so, to inform

organisations with whom we have shared your information that you have made a request for erasure.

The right to restrict processing

You have the right to ask us to restrict processing of your personal data in the following circumstances:

If you contest the accuracy of your personal information and we need to verify its accuracy If we have unlawfully processed your information and you do not want us to erase the data If we no longer need your information but you need to keep it in order to establish, exercise or defend a legal claim You have objected to us processing your information and we are considering whether we have legitimate grounds to continue to process it

This right to restrict processing is closely linked but is distinctly different from the right to rectification and the right to object. As a matter of good practice we may automatically restrict processing of your personal information while we consider its accuracy or the legitimacy of processing it.

The right to data portability

You have a right to receive personal data that you have provided to us in order to transfer it onto another data controller. This right only applies where the processing is based on consent and is carried out by automated means. This is called a data portability request.

The right to object

You have the right to object to our processing your personal information where our lawful basis for processing is based on the performance of a 'public task' carried out in the public interest or exercise of official authority.

You have the right to withdraw your consent to our processing your personal information if our lawful basis for processing is 'consent'.

You also have the right to object to processing for the purpose of direct marketing. You can opt-out of receiving marketing communications from us at any time. You can do this by clicking on the 'unsubscribe' or 'opt-out' link in marketing emails we send to you. If you wish to opt-out of other forms of marketing such as postal or telephone marketing contact us using the addresses or telephone number below.

If we are processing your personal information for scientific or historical research, or statistical purposes your right to object is more limited.

How to Withdraw Consent

Where we are processing your or your child's personal data based on consent, you have the right to withdraw that consent at any time.

To withdraw consent, please:

1. Contact your child's school office in writing (by email or letter)
2. Clearly state what consent you are withdrawing (e.g., "I withdraw consent for photographs of my child to be used on the school website")
3. Provide your child's name and class

We will action your request as soon as possible and confirm when the change has been made. Please note that withdrawing consent does not affect any processing that took place before you withdrew consent.

The right of complaint or to raise a concern

You have the right to raise a concern or make a complaint about how we handle (process) your personal information or if you are not satisfied with how we have dealt with a request.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact the Trust's Chief Operating Officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, in the first instance, please contact the Trust's Chief Operating Officer. Beaconfields Primary School, Ramson Avenue, Stafford, Staffordshire. ST16 1ZY. 01782 228912 Email: lausten@creativelrng.com

The Data Protection Officer acting for the Trust is:

Hedda Motherwell
Staffordshire County Council
Staffordshire Place 1
Stafford, Staffordshire
ST16 2DH
Telephone: 01785 278717

Email: dpo@staffordshire.gov.uk

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this Trust.