



ALDER GRANGE SCHOOL

Third Party Policies

Parent Pay

In order to carry out these services, we obtain (either from the Customer and/or from you directly) and process the following information:

Data Subject (Who)	Data Category (What)	Description
Pupil \ Student Forename	This is the forename of the pupil.	
Pupil \ Student Surname	This is the surname of the pupil.	
Pupil \ Student Known as	This is the name that the pupil is known as.	
Pupil \ Student DOB	This is the date of birth of the pupil.	
Pupil \ Student Gender	This is the pupil's gender	
Pupil \ Student Groups	Registration group (if any), year, other groups	
Pupil \ Student Salutation	This is the pupil's salutation.	
Pupil \ Student Dietary Requirements	This is the pupil's special dietary requirements	
Pupil \ Student Postal Address	The student's postal address	
Pupil \ Student Identifiers	Roll/Admission number, UPN, management system identifier	
Pupil \ Student Meal Selections	and spend history this is a history of a pupil's meal selections and spends for school meals or non-meal-related items, including free school meals	
Pupil \ Student Trip information	Trip details collected from parents, e.g. emergency contacts, medical details, dietary requirements, doctor's contact, EHIC and Passport	
Parent's \ Contacts Title	This is the contact's title (Mr, Mrs, Ms, etc.).	
Parent's \ Contacts Forename	This is the contact's forename.	
Parent's \ Contacts Surname	This is the contact's surname.	
Parent's \ Contacts Authentication data	Username and password, single-sign-or multi-factor-authentication tokens	
Parent's \ Contacts Gender	The contact's gender (Salutation)	
Parent's \ Contacts House Name	The text entered as the contact's house name.	
Parent's \ Contacts Street	the text entered as the contact's street.	
Parent's \ Contacts Locality	The text entered as the contact's locality.	
Parents \ Contacts Town	The text entered as the contact's town.	
Parent's \ Contacts Postcode	The text entered as the contact's post code.	
Parent's \ Contacts Day Telephone	The contact's daytime telephone number.	
Parents \ Contacts Home Telephone	The contact's home telephone number. Parent's \ Contacts Mobile Telephone This is the contact's mobile telephone number used to receive alerts from Parentpay and for school communications	
Parents \ Contacts Email	This is the contact's E-mail address used to receive communications from Parentpay and for school communications.	
Parent's \ Contacts Payment History	and balances this is the contact's history of payment transactions, including reversals, refunds and withdrawals of funds.	
Parents \ Contacts Payment card details	Payment card details are captured and passed to a 3rd party for authorisation.	
Parent's \ Contacts Other	This is the contact's alternative communication method.	
Parents \ Contacts In-app messages	Messages sent from parents to school within the ParentPay application	
Parent's \ Contacts Trouble ticket data	when users submit trouble ticket information, this gets stored.	

Parent's \ Contacts Shop information	ParentPay can be used as a payment page from externally or internally hosted shop systems. This the information captured as part of that ("shopping basket").
Parents \ Contacts Browser Details	IP address, cookies, browser information
Parent's \ Contacts Scottish UPRN	For users in Scotland who sign up via MyGovScot
School Staff Title	This is the staff member's title (Mr, Mrs, Ms, etc.).
School Staff Forename	This is the staff member's forename.
School Staff Surname	This is the staff member's surname.
School Staff Gender	The staff member's gender
Website Access IP Address	The network address of your device or internet connection
Website Access Browser Type and Version	The type of Web Browser your device is using
Website Access Cookies	Special records in your browser to help the website operate
Website Access Web Analytics	Generalised information about browsing behaviour and page statistics

Parent Mail

ParentPay (Holdings) Limited ("ParentPay Group") through its subsidiaries ParentPay Limited, Nimbl Limited, Cypad Limited and Just Education Limited is engaged in the design, development, sales, marketing, supply, operation and maintenance of, in the case of ParentPay Limited ("PPL") and Cypad Limited, payment collection, payment processing, school meal management, parent communication and management information systems and services for the education market, in the case of Nimbl Limited, youth banking, payment and debit card issuing services, and, in the case of Just Education Limited, education recruitment services (together the "Group Products and Services").

This notice explains to ParentPay Users ("you/your") how ParentPay Group ("we/us") use your personal information.

This privacy notice covers:

- Why we use your personal information
- The legal basis for processing
- What personal information we use
- How we use your personal information
- Your rights under data protection legislation
- Sharing personal information with third parties
- How long we may keep your information
- Changes to our privacy notice
- Contact details for our Data Protection Officer

Why we use your personal information

The PPL payment solutions, catering systems and communication platforms ("PPL Products and Services"), which are marketed in the UK under the ParentPay, Schoolcomms and Cypad brands, are provided to schools and their parents governed by a contract between us and the schools, Multi-Academy Trust or a Local Education Authority ("ParentPay Customer"), and also the Terms and Conditions that you agree with when you sign up ("ParentPay User").

We process your personal data for the following purposes:

- to provide you with the service activated and registered for
- the verification of your identity where required
- for the prevention and detection of crime, fraud and anti-money laundering
- for the ongoing administration of the service
- to allow us to improve the products and services we offer to our customers
- to ask for your opinion about our products and offer surveys
- for research and statistical analysis including payment and usage patterns
- We only use the data in an anonymized manner when we use your data for this purpose.
- to enable us to comply with our legal and regulatory obligations
- to offer new products and services to you which are relevant and appropriate, and only to the extent that would be reasonably expected.

If we plan to introduce further processes for the use of your information, we will provide information about that purpose prior to such processing.

The legal basis for processing

Under Data Protection Law, there are various grounds which are considered to be a 'legal basis for processing'.

The legal basis for processing should be determined by the Data Controller.

Where we are the Data Processor, the legal basis is determined by the Customer. Typically, the legal basis in this scenario is:

'processing is necessary for the performance of a task carried out in the public interest'

and/or

'processing is necessary for the purposes of legitimate interests pursued by the controller'

Where we are the Data Controller, the legal basis for processing is based on:

'processing is necessary for the purposes of legitimate interests pursued by the controller'

It should be noted that in some circumstances this legal basis may vary, however, we always operate in full compliance with Data Protection Law and will only process data with a fair and reasonable legal basis for doing so.

What personal information we process

In order to carry out these services, we obtain (either from the Customer and/or from you directly) and process the following information: INSERT TABLE HERE

Data Subject (Who)	Data Category (What)	Description
Pupil \ Student	Forename	This is the forename of the pupil.
Pupil \ Student	Surname	This is the surname of the pupil.
Pupil \ Student	Known as	This is the name that the pupil is known as.
Pupil \ Student	DOB	This is the date of birth of the pupil.
Pupil \ Student	Gender	This is the pupil's gender
Pupil \ Student	Groups	Registration group (if any), year, other groups
Pupil \ Student	Salutation	This is the pupil's salutation.
Pupil \ Student	Dietary Requirements	This is the pupils special dietary requirements
Pupil \ Student	Postal Address	The student's postal address
Pupil \ Student	Identifiers	Roll/Admission number, UPN, management system identifier
Pupil \ Student	Meal Selections and spend history	This is a history of a pupil's meal selections and spends for school meals or non-meal-related items, including free school meals
Pupil \ Student	Trip information	Trip details collected from parents, e.g. emergency contacts, medical details, dietary requirements, doctor's contact, EHIC and Passport
Parents \ Contacts	Title	This is the contact's title (Mr, Mrs, Ms, etc.).
Parents \ Contacts	Forename	This is the contact's forename.
Parents \ Contacts	Surname	This is the contact's surname.
Parents \ Contacts	Authentication data	Username and password, single-sign-or multi-factor-authentication tokens
Parents \ Contacts	Gender	The contact's gender (Salutation)
Parents \ Contacts	House Name	The text entered as the contact's house name.
Parents \ Contacts	Street	The text entered as the contact's street.
Parents \ Contacts	Locality	The text entered as the contact's locality.
Parents \ Contacts	Town	The text entered as the contact's town.
Parents \ Contacts	Postcode	The text entered as the contact's post code.

Parents \ Contacts	Day Telephone	The contact's daytime telephone number.
Parents \ Contacts	Home Telephone	The contact's home telephone number.
Parents \ Contacts	Mobile Telephone	This is the contact's mobile telephone number used to receive alerts from Parentpay and for school communications
Parents \ Contacts	Email	This is the contact's E-mail address used to receive communications from Parentpay and for school communications.
Parents \ Contacts	Payment History and balances	This is the contact's history of payment transactions, including reversals, refunds and withdrawals of funds.
Parents \ Contacts	Payment card details	Payment card details are captured and passed to a 3 rd party for authorisation.
Parents \ Contacts	Other	This is the contact's alternative communication method.
Parents \ Contacts	In-app messages	Messages sent from parents to school within the ParentPay application
Parents \ Contacts	Message Status	We may record the 'opened' status of emails sent from the platform, via pixel tags
Parents \ Contacts	Trouble ticket data	When users submit trouble ticket information, this gets stored.
Parents \ Contacts	Shop information	ParentPay can be used as a payment page from externally or internally hosted shop systems. This the information captured as part of that ("shopping basket").
Parents \ Contacts	Browser Details	IP address, cookies, browser information
Parents \ Contacts	Scottish UPRN	For users in Scotland who sign up via MyGovScot
School Staff	Title	This is the staff member's title (Mr, Mrs, Ms, etc.).
School Staff	Forename	This is the staff member's forename.
School Staff	Surname	This is the staff member's surname.
School Staff	Gender	The staff member's gender
Website Access	IP Address	The network address of your device or internet connection
Website Access	Browser Type and Version	The type of Web Browser your device is using
Website Access	Cookies	Special records in your browser to help the website operate
Website Access	Web Analytics	Generalised information about browsing behaviour and page statistics

How we process your personal information

We use your personal information, and some of our employees have access to such information, only to the extent required to carry out the services for you and on behalf of the Customer.

We have introduced appropriate technical and organisational measures to protect the confidentiality, integrity and availability of your personal information during storage, processing and transit.

We are a Level 1 PCI-DSS certified organisation and are subject to regular and comprehensive security audits. We operate an ISO27001 compliant security programme to help protect your data at all times.

The PPL Products and Services only processes your personal information in the UK. Some of our supporting services (for example ZenDesk), might use cloud platforms that operate from Third Countries outside of the EEA. Where this is the case, we ensure that adequate safeguards are established to protect your data.

Your rights under Data Protection Law

Right to Access

You have the right of access to your personal information that we process and details about that processing.

You can usually access that information directly within the PPL Products and Services (self-service). However, should this not be possible, you can raise a Data Subject Access Request (DSAR) to receive this information in another format.

Right to Rectification

You have the right to request that information is corrected if it's inaccurate. You can usually update your own information using the PPL Products and Services (self-service). However, should this not be possible, you can contact us to make the changes on your behalf. In some circumstances, you may have to contact your child's school, to correct the data held by them and provided to us for processing.

Right to Erasure (Right to be Forgotten)

You have the right to request that your information is removed; depending on the circumstances, we may or may not be obliged to action this request.

Right to Object

You have the right to object to the processing of your information; depending on the circumstances, we may or may not be obliged to action this request.

Right to Restriction of Processing

You have the right to request that we restrict the extent of our processing activities; depending on the circumstances, we may or may not be obliged to action this request.

Right to Data Portability

You have the right to receive the personal data which you have provided to us in a structured, commonly used and machine readable format suitable for transferring to another controller.

Right to lodge a complaint with a supervisory authority

If you think we have infringed your privacy rights, you can lodge a complaint with the relevant supervisory authority. You can lodge your complaint in particular in the country where you live, your place of work or place where you believe we infringed your right(s).

You can exercise your rights by sending an e-mail to dpo@parentpay.com. Please state clearly in the subject that your request concerns a privacy matter, and provide a clear description of your requirements.

Note: We may need to request additional information to verify your identity before we action your request.

Sharing personal information with third parties

We use a range of trusted service providers to help deliver our services. All of our suppliers are subject to appropriate safeguards, operating in accordance with our specific instructions and limitations, and in full compliance with Data Protection Law.

These service providers include:

- Payment Processors – to securely process your card payments (we do not see, or store payment card details)
- SMS Providers – to send out our SMS notifications or messages sent by Customers using PPL Products and Services
- Email Providers – to send out our email notifications or messages sent by Customers using PPL Products and Services
- Hosting Providers – to manage our secure enterprise datacentres
- Security Providers – to protect our systems from attack
- Telephony Providers – we might record calls for training, quality and security purposes
- Training Platforms – to train school staff on the use of our services
- Support Portal (ZenDesk) – so that you can easily ask for help

- Bank Transfer functionality – working with Corvid and Experian
- Cloud Hosting and Recovery – working with AWS and Azure
- Security insight and system logging – working with Rapid7
- Cloud email delivery – working with Sendgrid (USA hosted)
- Anonymous Web Analytics – working with Google
- Feedback Platforms (Optional) – working with Survey Monkey

We may also have access to your personal information as part of delivering the service. If we need to change or add additional third parties, we will always update our Privacy Notice accordingly. We will only disclose your information to other parties in the following limited circumstances

- where we are legally obliged to do so, e.g. to law enforcement and regulatory authorities
- where there is a duty to disclose in the public interest
- where disclosure is necessary to protect our interest e.g. to prevent or detect crime and fraud
- where you give us permission to do so e.g. by providing consent within the PPL Products and Services or via an online application or consent form

How long we may keep your personal information

We will only retain information for as long as is necessary to deliver the service safely and securely. We may need to retain some records to maintain compliance with other applicable legislation – for example finance, taxation, fraud and money laundering law requires certain records to be retained for an extended duration, in some cases for up to seven years.

Pupil data will typically be removed or anonymised when the following rules are met:

- The pupil has been archived by the School for longer than one month.
- The pupil does not have any meal consumption or attendance data within the last 13 months.
- The pupil has not received a payment for any payment item within the last 13 months.
- The pupil balance is zero.

Payer (Parent) data will usually be removed or anonymised when the following rules are met:

- They have not logged in for 13 months.
- They have not topped up or spent within the last 13 months.
- Parent balance is 0 (zero), and all pupil balances are 0 (zero).
- There are no active pupils associated with the account

Manager Accounts that have been disabled and have not logged in for 13 months, will be removed or anonymised. Other school staff accounts are subject to the same rules as pupils (above)

Message attachments will be removed after 24 months.

File area uploads will be purged after 24 months.

Personal information in trip records will be removed 1 month after trip completion

It should be noted that Schools will still retain a complete finance audit trail for their statutory requirements. In unusual cases where specific personal information needs to be retained, then this can be facilitated upon request.

Changes to our Privacy Notice

This policy will be reviewed regularly and updated versions will be posted on our websites.

Contact details for our Data Protection Officer

We have appointed a Data Protection Officer (DPO); their contact details are as follows:

dpo@parentpay.com

or

Data Protection Officer

ParentPay

Ricoh Arena

Phoenix Way

Coventry

CV6 6GE

VeriCool

Vericool Ltd will only use the information that we collect lawfully and in accordance with the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act (2018). Vericool Ltd will always offer you the chance to refuse any marketing email from us. We do not sell, rent or trade personal information to third parties for marketing purposes.

We will comply with the Data Protection legislation, so any personal data which you supply to us will be used for the sole purpose indicated on the relevant section of the website, for example to send you an advisory note or provide you with any other requested service. We will not store any personal data of any sort without your express permission.

The information we hold about you is confidential and will only be used to investigate or prevent fraud or if the law permits it or it is in the public interest.

We will only retain your personal data only for as long as is required and for the purposes for which it was originally given. The personal details are then destroyed unless we are legally obliged to retain the data and/or transmit it to a regulatory or government authority.

We would ask that you keep us informed (by email, telephone, or in writing) of any changes in your personal data so that we may have our records up to date at all times.

We will from time to time amend this Privacy Policy and Data Protection Statement and such amendments will be posted on the website.

Upon payment of a fee and by written request to Vericool Ltd, you are entitled to a copy of the personal data held about you by us, as provided for under GDPR. You also have the right to require us to correct any inaccuracies in your information.

We may use technology to track the patterns of behaviour of visitors to our site. This can include using a 'cookie' which would be stored on your browser. You can usually modify your browser to prevent this happening. The information collected in this way can be used to identify you unless you modify your browser settings.

Biometric data and GDPR

Unless specifically agreed with the customer, Vericool does not hold biometric data nor does it have access to it. All biometric data is held on a client server under control of the client and based within the clients firewall and network. Vericool has no access to this data.

Notwithstanding the above Vericool is committed to following framework:

The EU GDPR establishes a harmonized framework within the European Union, the right to be forgotten, clear and affirmative consent and, amongst other things, serious penalties for failure to comply with these rules.

The Regulation 2012/0011 was adopted officially on 27 April 2016 It came into force on 24 May 2016 Member States had to transpose it into their national law by 6 May 2018 The provisions of the Regulation are applying as of 25 May 2018.

What is biometric data for the EU regulation? The EU data privacy law defines biometric data as "special categories of personal data" and prohibits its "processing".

More precisely, biometric data are "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data".

The Regulation protects EU citizens and long-term residents from having their information shared with third parties without their consent. Their processing for "uniquely identifying a natural person" is prohibited. However, it does contain some exceptions: •If consent has been given explicitly

•If biometric information is necessary for carrying out obligations of the controller or the data

subject in the field of employment, social security and social protection law •If it's necessary to protect the vital interests of the individual and he/she is incapable of giving consent •If it's vital for any legal claims •If it's necessary for reasons of public interest in the area of public health. Moreover, the Regulation permits Member States to introduce other limitations regarding the processing of biometric information.

General note on GDPR for Schools re Vericool Ltd Vericool Ltd is a provider of cashless catering and registration systems to schools. Vericool has a comprehensive internal policy on GDPR and has conducted a detailed audit together with staff training to ensure compliance.

With the exception of our payment portal (please see details below) no third party data is held by Vericool Ltd. All data for our systems is held in an encrypted sql on the school central database, to which Vericool does not have access without the explicit permission of the school.

On very rare occasions and with the explicit permission of the school we may bring some data back to Vericool. In the unlikely event this was necessary we have a dedicated and secure server. This server has a range of security measures including it not being connected to the internet, internally it is held within its own vlan. All data is hard deleted as soon as it is finished with and it is our policy to physically destroy the hard disk once a year.

We do not share any information with any third parties and conduct no marketing or data analysis using it.

Payment portal A number of customers use the Vericool dedicated payment portal.

Vericool maintains a payment portal in an encrypted data base at a high security data centre. The following information is retained for as long as it is required. The length of retention is reviewed from time to time.

Student:

Email address

FirstName

LastName

Year Group

Reg Code

Admission Number

Meal Transactions made in schools

Parents:

Email Address

Password

No credit card information is held by Vericool Ltd

BKSB

1. Introduction

- We are committed to safeguarding the privacy of our website visitors and service users; in this policy we explain how we will handle your personal data.
- By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.
- We will always hold your information securely and to prevent unauthorised disclosure or access to your information, we have implemented strong physical and electronic security safeguards.
- This policy is updated from time to time. The latest version is published on this page. This website privacy policy was updated on 28/7/20.

2. Credit

- This document was created using a template from SEQ Legal (<http://www.seqlegal.com>).

3. How we use your personal data

- In this Section 3 we have set out:
 4. the general categories of personal data that we may process;
 5. in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
 6. the purposes for which we may process personal data; and
 7. the legal bases of the processing.
- We may process data about your use of our website and services ("**usage data**"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis for this processing is our legitimate interests, namely monitoring, protecting and improving our website and services.
- We may process information contained in any enquiry you submit to us regarding products and/or services. ("**enquiry data**"). The enquiry data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website forms. The enquiry data may be processed for the purposes of offering, marketing and selling relevant products and/or services to you. The legal basis for this processing is our legitimate interests, namely the proper administration of our business and communications with customers
- We may process information contained in or relating to any communication that you send to us ("**correspondence data**"). The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact form. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our business and communications with customers.
- We may process eNewsletter subscription data that you send to us ("**subscription data**"). The subscription data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website eNewsletter form. This data may be processed for the purposes of sending you an eNewsletter from time to time. The legal basis for this processing is consent.
- We may process data regarding your registration for an event/conference/webinar you submit to us. ("**event data**"). The data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website forms. The data (except for any 'special category data') may be processed for the purposes of registering for, and the administration of, the event/conference/webinar. The legal basis for this processing (except for special category data) is our legitimate interests, namely the proper administration of our events and communications with attendees. Where we process 'special category' data for an event/conference/webinar related to dietary requirements or other health needs, the legal basis for this processing will be consent.
- We may process any of your personal data identified in the other provisions of this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.

- In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.
 - Please do not supply any other person's personal data to us, unless we prompt you to do so.
- 8. Providing your personal data to others**
- In this Section 4, we provide information about the circumstances in which your personal data may be shared with others.
 - We may disclose your personal data to our professional advisers insofar as reasonably necessary for the purposes of managing risks, obtaining professional advice, or the establishment, exercise or defense of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
 - We may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.
- 9. International transfers of your personal data**
- In this Section 5, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA).
 - The personal data we collect from you may be transferred to, shared and/or otherwise processed by organisations or companies outside the United Kingdom or the European Economic Area ("EEA"). Where your personal data is transferred outside the UK or EEA, we will take steps to ensure that the recipient implements appropriate measures to protect your personal data (for example, by entering into EU Commission approved standard contractual clauses), as required under the applicable data protection laws.
 - bksb uses a variety of online services such as **Mail Chimp** (www.mailchimp.com – a popular web-based email marketing service for communicating with our customers). When you/we enter your personal details into these websites, the hosting facilities for these sites may be situated in the USA. The European Commission has made an "adequacy decision" with respect to the protection afforded by the EU-Swiss Privacy Shield (to which Mail Chimp comply). Transfers to the USA will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission, a copy of which you can obtain from https://ec.europa.eu/info/sites/info/files/celex_32016d1250_en_txt.pdf.
 - Copies of their privacy policies can be downloaded from their respective websites.
- 10. Retaining and deleting personal data**
- This Section 6 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.
 - Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
 - We will retain and delete your personal data as follows:
11. If you are a customer, or are taking steps to become a customer, we will retain your data for communication and marketing purposes until at such time you notify us you no longer wish to receive this information. You can unsubscribe from our eNewsletter at any time.
12. All personal data we gather via any forms is reviewed on at least an annual basis and deleted if no longer required.
13. Special category data gathered during the registration process for an event/conference will be deleted after the event has taken place.
- Notwithstanding the other provisions of this Section 6, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.
- 7. Amendments**
- We may update this policy from time to time by publishing a new version on our website.
 - You should check this page occasionally to ensure you are happy with any changes to this policy.
 - We may notify you of changes to this policy by email or through the notifications system on our website.
- 8. Your rights**
- In this Section 8, we have summarised the rights that you have under the General Data Protection Regulations (GDPR). Some of the rights are complex, and not all of the details have been included

in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

- Your principal rights under data protection law are:
- 9. the right to be informed;
- 10. the right of access;
- 11. the right to rectification;
- 12. the right to erasure;
- 13. the right to restrict processing;
- 14. the right to data portability;
- 15. the right to object to processing;
- 16. the right to object;
- 17. rights related to automatic decision making and profiling.
 - **Right to be informed** – You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data.
 - **Right of access** – Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data at no cost.
 - **Right to rectification** – You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.
 - **Right to erasure** – In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; or the personal data has been unlawfully processed. However, there are certain general exclusions of the right to erasure. Those general exclusions include where processing is necessary for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.
 - **Right to restrict processing** – In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it, with your consent, for the establishment, exercise or defence of legal claims, for the protection of the rights of another natural or legal person, or for reasons of important public interest.
 - **Right to data portability** – You have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.
 - **Right to object** – You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.
 - **Rights related to automatic decision making and profiling** – You have the right to object to automatic decision making or profiling based on your personal data that has a legal or similarly significant effect.
 - You may exercise any of your rights in relation to your personal data by written notice to us. *Contact details for the data protection officer can be found at the end of this document.*

18. About cookies

- bksb Limited is committed to protecting you and any data (anonymous or otherwise) that we collect about you online. This section tells you how we use cookies, why, and how this allows us to improve our service. It also tells you how you can manage what cookies are stored on your device. We call it our Cookies Policy.
- By using our website (through any device) you agree that this Cookies Policy applies to that use in addition to any other terms and conditions which may apply.
- We reserve the right to make changes to our Cookies Policy. Any changes will appear here and become effective immediately. Your continued use of our website is taken as meaning that you agree to such changes.

19. What are Cookies?

- Cookies are files containing small amounts of information which are downloaded to the device you use when you visit a website. Cookies are then sent back to the originating website on each subsequent visit, or to another website that recognises that cookie. Cookies do lots of different and useful jobs, such as remembering your preferences, and generally improving your online experience.
- We use Google Analytics to analyse the use of the website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. The relevant cookie is `_ga`. This cookie contains no personal information that can be used to identify an individual.
- Cookies will also be placed onto your computer to remember your preferences and other information, such as your preferred language (e.g. English), how many search results you wish to have shown per page, and whether or not you wish to have Google's SafeSearch filter turned on. When you play an embedded YouTube video, cookies help to ensure the video is delivered at a quality that best matches your available bandwidth. The relevant cookies are `PREF`, `NID` and `Visitor_INFO1_LIVE`. These cookies contain no personal information that can be used to identify an individual.
- More information about Google's privacy policy is available at: <https://www.google.com/policies/privacy>

11. What if I don't want to accept cookies?

- Blocking all cookies will have a negative impact upon the usability of many websites.
- If you block cookies, you will not be able to use all the features on our website.

12. Managing cookies?

- You can allow cookies from specific websites by making them "trusted websites" in your Internet browser and for more information on how to do this in popular web browsers (Internet Explorer, Google Chrome, Firefox and Safari), go to [All about cookies](#).

13. Our details

- This website is owned and operated by bksb Limited.
- We are registered in England and Wales under registration number 03311079, and our registered office is at bksb Limited, I2 Centre, Hamilton Court, Hamilton Way, Mansfield, Notts, NG18 5FB.
- Our principal place of business is at bksb Limited, I2 Centre, Hamilton Court, Hamilton Way, Mansfield, Notts, NG18 5FB.
- You can contact us:

14. by post, using the postal address given above;

15. using our website contact form;

16. by telephone, on the contact number published on our website; or

17. by email, using the email address published on our website.

18. If your reason to contact us is to obtain information under your right of access, please request a copy of our *Subject Access Request Form*

19. Data protection officer

- Our data protection officer's contact details are:

20. by mail: Data protection officer, bksb Limited, I2 Centre, Hamilton Court, Hamilton Way, Mansfield, Notts, NG18 5FB;

21. by email: dpo@bksb.co.uk;

22. by telephone, on the contact number published on our website.

Fisher Family Trust

Welcome to the privacy notice of FFT Education Limited (**FFT**).

This notice tells you what we do with personal data relating to the users of our services as well as data that is processed by us in providing those services, in particular the personal data of pupils of schools in England and Wales. It also tells you what we do with personal data collected through our websites, including cookies and applications submitted through website forms.

FFT takes your privacy very seriously. We ask that you read this privacy notice carefully as it contains important information about what to expect when we collect and process your personal data and how we will use your personal data.

These websites fft.org.uk, fftaspire.org, analytics.fftaspire.org, ffteducationdatalab.org.uk, training.fft.org.uk and fft.peoplehr.net (the **websites**) are operated by FFT, a not-for-profit limited liability company incorporated in England and Wales under company number 03685684, with its head office at 1st Floor, 79 Eastgate, Cowbridge, Vale of Glamorgan CF71 7AA.

These websites are not intended to be used by children.

FFT Aspire is a well-established service provided to schools and organisations that support them (Local Authorities, Multi Academy Trusts and Diocese) to help schools to improve educational outcomes through the use of data. Aspire can be accessed through the websites fftaspire.org and analytics.fftaspire.org. It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing your personal information so that you are fully aware of how and why we are using your data. This privacy notice supplements any other notices and is not intended to override them.

This privacy notice is provided in a layered format so you can click through to the specific areas set out below.

[Data controller and how to contact us](#)

[Your duty to inform us of changes](#)

[The information we collect about you](#)

[How is your personal data collected?](#)

[How we will use your data](#)

[When we will disclose your data to third parties](#)

[Marketing](#)

[Cookies and other information-gathering techniques](#)

[How we protect your data](#)

[Overseas transfers](#)

[Your rights](#)

[Links to other sites](#)

[Changes to our privacy notice](#)

Data controller and how to contact us

FFT is the data controller and responsible for your personal data (collectively referred to in this privacy notice as FFT, “we” “us” or “our”).

Some of the personal data we process is provided to us on behalf of third party data controllers including the Department for Education or our customers, which include local authorities, academy trusts, dioceses and schools. In some circumstances we will only be the processor of that data and in other circumstances we will also be a controller of that data.

We have appointed a data protection officer for overseeing questions in relation to privacy matters. If you have any questions about this privacy notice, including any requests to exercise your data protection rights, please contact them using the details set out below.

Email: dpo@fft.org.uk

Phone: 01446 776 262

Write: Helen Robinson (DPO), FFT Education Ltd, 1st Floor, 79 Eastgate, Cowbridge, Vale of Glamorgan, CF71 7AA.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

Your duty to inform us of changes

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example if you are a user of the Aspire platform and you change your email address.

The information we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you, such as:

- **Identity Data** includes first name, last name, username, email address and job title.
- **Contact Data** includes employer, work address, country of residence, phone number, email address and telephone numbers.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, settings, cookie data, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our websites and the Aspire service.
- **Profile Data** includes your username and password, interests, preferences, feedback, survey responses and training received.
- **Usage Data** includes information about how you use our websites and services, including areas of Aspire accessed, analyses viewed and updates made.
- **Marketing and Communications Data** includes your preferences in receiving marketing communications and your communication preferences.
- **Careers Data** includes information provided in applying for a role through fft.peoplehr.net, including job history and other CV data in addition to Identity Data and Contact Data.
- **DfE Pupil Data** provided to us by the Department for Education about current and former school pupils including name, data of birth, gender, language, ethnicity, school(s) attended and the home census output area, school exam and assessment information, any special educational needs and attendance and absence information.
- **Customer Pupil Data** includes information obtained from schools and organisations supporting schools (such as local authorities, academy trusts, dioceses and other education providers) including, in addition to pupil data provided by the DfE, details of which pupils are on-roll, absence information, pupil estimates and targets, teacher assessments, assessment results from tests, allocation to pupil groups and data in respect of which teachers taught particular pupils.

We may also use aggregate information and statistics for the purposes of monitoring website usage in order to help us to develop our website and our services. Aggregate information may be derived from your personal data but is not considered personal data in law as this data does not directly or indirectly reveal your identity. We may also provide such aggregate information to third parties. If we do combine or connect any aggregate information with your personal data so that it can identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any **Special Categories of Personal Data** about users (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

The DfE Pupil Data and Customer Pupil Data we process does include **Special Categories of Personal Data**. This data (including language, ethnicity and information about special educational needs) is used to help customers to ensure that all of their pupils are given equality of opportunity and treatment. For example, it may be used to create "value added" models to compare the progress of pupils with similar characteristics in different schools. The legal basis of processing is covered by the Data Protection Act 2018, Schedule 1, part 2, paragraph 8 (Substantial Public Interest Conditions – Equality of opportunity or treatment).

How is your personal data collected?

We use different methods to collect data from and about you, including through:

- **Direct communications.** When you input your details to set up a user account or ask for support we collect your Identity Data, Contact Data and Profile Data.

- **From your employer.** FFT customers provide information about their users of Aspire to FFT which may include Identity Data, Contact Data and Profile Data.
- **From the Department for Education.** The Department for Education provides DfE Pupil Data subject to agreements with FFT.
- **Customer data.** Schools, local authorities, academy trusts, dioceses and other education providers provide Customer Pupil Data to be added to Aspire in their use of the service, subject to the terms of contracts between the customer and FFT.
- **Automated technologies.** As you interact with our websites, we automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data using cookies, server logs and other technologies. Please see section 8 below and our [Cookies Policy](#) for further details.

How we will use your data

We have set out in the table below a description of the ways we plan to use your personal data and which legal bases we rely on to do so. We have identified what our legitimate interests are where appropriate.

Purpose/activity	Type of data	Lawful basis for processing including basis of legitimate interest
To allow schools and organisations who support schools (such as local authorities, academy chains and dioceses) to analyse pupil data and related analyses via the Aspire portal	<input type="checkbox"/> DfE Pupil <input type="checkbox"/> Customer Pupil	<input type="checkbox"/> Necessary for our customers' legitimate interests (analysis of pupil performance, school performance, staff performance and ensuring equality of opportunity and treatment of pupils) <input type="checkbox"/> Necessary for our legitimate interests (provision of our core services to customers)
To create and apply models to analyse past and future pupil performance	<input type="checkbox"/> DfE Pupil <input type="checkbox"/> Customer Pupil	<input type="checkbox"/> Necessary for our customers' legitimate interests (analysis of pupil performance and requirements, school performance, staff performance and ensuring equality of opportunity and treatment of pupils) <input type="checkbox"/> Necessary for our legitimate interests (provision of our core services to customers)
To produce research outputs including research papers and educational blogs	<input type="checkbox"/> DfE Pupil <input type="checkbox"/> Customer Pupil	<input type="checkbox"/> Necessary for our legitimate interests (marketing, provision and improvement of our core services to customers)
To register you as a user of Aspire	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Usage <input type="checkbox"/> Technical	<input type="checkbox"/> Necessary for our legitimate interests (provision of our core services to your school/employer)
To process and deliver invoices to customers and to evidence use by customers	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Usage <input type="checkbox"/> Technical	<input type="checkbox"/> Performance of a contract with you <input type="checkbox"/> Necessary for our legitimate interests (to administer and recover amounts owing to us, to defend or pursue legal claims in respect of usage of Aspire)
To evidence use by customers	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Usage <input type="checkbox"/> Technical	<input type="checkbox"/> Necessary for our legitimate interests (to defend or pursue legal claims in respect of the usage of Aspire, to maintain evidence in respect of pupil safeguarding requirements)
To manage our relationship with you which will include:	<input type="checkbox"/> Identity <input type="checkbox"/> Contact	<input type="checkbox"/> Necessary to comply with a legal obligation <input type="checkbox"/> Necessary for our legitimate interests (to keep our

Purpose/activity	Type of data	Lawful basis for processing including basis of legitimate interest
(a) Notifying you about changes to our terms or privacy notice (b) Asking you to leave a review or take a survey	<input type="checkbox"/> Profile <input type="checkbox"/> Marketing and Communications	records updated and to study how customers and users use our products/services)
To provide helpdesk, support and maintenance services to users of Aspire	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Usage	<input type="checkbox"/> Performance of a contract with you <input type="checkbox"/> Necessary for our legitimate interests (provision of our core services to your school/employer)
To make suggestions and recommendations to you about products or services that may be of interest to you	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Marketing and Communications	<input type="checkbox"/> Necessary for our legitimate interests (to develop our products/services and grow our business)
To review your application for a job	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Careers	<input type="checkbox"/> Necessary for our legitimate interests (to evaluate you as a prospective job candidate and contact you in that respect)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Technical <input type="checkbox"/> Usage <input type="checkbox"/> Profile	<input type="checkbox"/> Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) <input type="checkbox"/> Necessary to comply with a legal obligation
To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Usage <input type="checkbox"/> Technical	<input type="checkbox"/> Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile <input type="checkbox"/> Technical <input type="checkbox"/> Usage	<input type="checkbox"/> Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy) <input type="checkbox"/>
To record what training courses you have attended and offer other related services	<input type="checkbox"/> Identity <input type="checkbox"/> Contact <input type="checkbox"/> Profile	<input type="checkbox"/> Necessary for our legitimate interests (to promote our services and grow our business) <input type="checkbox"/> Necessary for our customers' legitimate interests (to ensure staff are suitably trained)
To undertake research into how education systems function	<input type="checkbox"/> DfE Pupil <input type="checkbox"/> Customer Pupil <input type="checkbox"/> Contact <input type="checkbox"/> Profile	<input type="checkbox"/> Necessary for our customers' legitimate interests (analysis of pupil performance and requirements, school performance, staff performance and ensuring equality of opportunity and treatment of pupils) <input type="checkbox"/> Necessary for our legitimate interests (to be able to

Purpose/activity	Type of data	Lawful basis for processing including basis of legitimate interest
		undertake research for public benefit)

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

We will retain and process your data for as long as we require it for the purposes for which it was collected or as is otherwise required by applicable law. To determine the appropriate retention period for your personal data, we consider the amount, nature and sensitivity of the personal data, the risk of potential harm from its unauthorised use or disclosure, the purposes for which we process it, whether we can achieve our purposes through other means, and the applicable legal requirements.

In respect of Pupil Data provided by the DfE, we will:

- Remove identifying information at the end of the academic year in which the learner reaches age 21.
- Delete the data no later than the end of the academic year in which the learner reaches age 23.
- In full, within 20 working days of termination of our contract with the Department for Education.

In respect of Customer Data, we will delete the data no later than 48 months after termination of the customer's subscription term.

In respect of the data of Aspire users, we will delete this data:

- 7 years after termination or expiry of the relevant Aspire subscription.
- 7 years after the subscribing organisation has deleted the relevant user from Aspire.

Once your personal data is no longer needed, we will securely delete or anonymise it. We may continue to use anonymised data, which cannot be associated with you, for research or statistical purposes.

When we will disclose your data to third parties

We will not sell, exchange or otherwise distribute your personal data to unaffiliated third parties without your consent, except to the extent required by applicable laws and regulations, or as set out in this privacy notice.

We may share data we collect with any related company (or other incorporated or unincorporated entity) within our corporate group and with selected third parties including:

- our UK partners (including local authorities, academy trusts and dioceses), where we enter into agreements to support the provision of services to schools;
- Other business partners, in order to provide our services (for example where we enter into agreements with third parties who provide services to us or on our behalf); and
- analytics and search engine providers that assist us in the improvement of our website and the services we provide.

We may also disclose data we collect to third parties:

- if we undergo a change of control or any of our business or assets are sold or transferred (in which case we may disclose your data to the prospective seller or buyer);
- if we or substantially all of our assets are acquired by a third party, in which case information held by us about our website users will be one of the transferred assets; or
- if we are under a duty to disclose or share your information in order to comply with any legal obligation or legal process (for example, a court order), or in order to enforce or apply our contractual rights or any other agreement; in order to protect the rights, property, or safety of our website users, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

Local authorities have access to school user data for administrative purposes where the school has subscribed to Aspire through that local authority.

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us. We may use your Identity, Contact, Marketing and Communications, Usage and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you. You will receive marketing communications from us if you have requested information from us, are a customer or user of our services, or we have obtained your business contact details as a prospective customer from elsewhere (including your employer's website or a directory) and, in each case, you have not opted out of receiving that marketing.

Opting out. You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you or by contacting us at any time.

Cookies and other information-gathering techniques

Our website uses cookies. Cookies are text files placed on your computer to collect standard Internet log information and visitor behaviour information. These cookies allow us to distinguish you from other users of our website which helps us to provide you with a good experience when you browse our website and also allows us to improve our site.

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our website may become inaccessible or not function properly.

For more information on our use of cookies, see our [Cookies policy](#) on our website.

How we protect your data

We will use all reasonable efforts to safeguard your personal data and we have put in place security procedures and technical and organisational measures to do so, including encryption. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

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

Overseas transfers

We do not transfer, or allow the transfer by our external processors, of pupil data outside of the UK.

Some of our external third parties (for example, the provider of our customer management system) are based outside the European Economic Area (**EEA**) so their processing of your personal data (other than pupil data) will involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We may transfer your personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission.
- Where we use certain service providers, we may use specific contracts approved by the European Commission which give personal data the same protection it has in Europe.
- Where we use providers based in the US, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA.

Your rights

In some circumstances you have rights in relation to the personal data we hold about you. Please [contact us](#) using the contact details above if you wish to exercise any of these rights.

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent** at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent

You will not usually have to pay a fee to exercise these rights but if your request is clearly unfounded, repetitive or excessive, we may charge a reasonable fee (or refuse to comply with your request).

We may need specific information from you to help us confirm your identity and to speed up our response; this helps keep your personal data safe and speeds up our response to your request. We try to respond to all legitimate requests within one month but this period may be longer if your request is particularly complex or you have made multiple requests; we will notify you in this case.

If we are only a data processor in respect of the data to which your request relates, we may not be able to comply with that request and will redirect you to the relevant data processor.

Links to other sites

Our websites may contain links to other sites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third party websites and are not responsible for their privacy statements. This privacy notice applies only to this website so when you access links to other sites you should read the privacy notice applicable to that site.

Changes to our privacy notice

We keep this privacy notice under regular review. If we change our privacy notice, we will post the changes on this page, and may place notices on other pages of the website, so that you may be aware of the information we collect and how we use it at all times.

School Cloud

GDPR Compliance Statement

The new General Data Protection Regulation (GDPR) brings new responsibilities to both data controllers and data processors who offer services to people within the European Union (EU). SchoolCloud are committed to high standards of data security and privacy. We have taken steps to ensure our services comply with the GDPR as of 25th May 2018.

In this article

- [Overview](#)
- [Data held on SchoolCloud Parents Evening](#)
- [Features to help comply with GDPR](#)
- [Data held about Schools](#)

Overview

We've always taken data security and data privacy very seriously. We welcome the new GDPR as we believe it clarifies individual privacy rights and brings greater responsibilities onto organisations who control or process data.

The GDPR brings new regulations on how organisations manage personal data. Personal data is any information which could be used directly or indirectly to identify a person.

How we've prepared for GDPR

- We've identified the personal data held and collected on our systems and undertaken a review to ensure this is appropriate for the service we offer.
For example: we've removed the parent phone number from the system. Although it was useful to see in order to follow-up with parents, it wasn't directly used by the system.
- We've made changes to how data is removed from SchoolCloud Parents Evening to satisfy the Right to Erasure.
- We've updated our [Terms & Conditions](#), and [Privacy Notice](#) to include appropriate clauses for GDPR which is effective from 25th May 2018.
- We've introduced a new [End-User Privacy Notice](#) which is effective from 25th May 2018.
- We've coordinated with our suppliers to ensure we have agreements with them which include appropriate clauses for GDPR.

Data held on SchoolCloud Parents Evening

We act as **data processors** for any data held on SchoolCloud Parents Evening by you, your school, or end-users of your school (such as parents or teachers). Personal data includes, but is not limited to: student data, teacher data, and parent data. It is your obligation as the data controller to ensure there is lawful basis for processing. We do not share this data with third-parties, though we may access this data as part of making improvements to our service and providing support to schools when requested.

We also act as **data controllers** when we create aggregated statistical data which may be derived from personal data, but is not considered personal data in law as it cannot be used directly or indirectly to identify a person.

What personal data we hold

- Student Data: first name, surname, registration class, date of birth, year group, MIS ID
- Contact Data: title, first name, surname, relationship to student, parental responsibility to student, contact priority to student, email address, MIS ID
- Teacher Data: title, first name, surname, email address, MIS ID

Where data is held

All data held on SchoolCloud Parents Evening is within the European Economic Area (EEA). We do not transfer this data outside of the EEA.

We host with one of the top managed hosting providers in the United Kingdom. We maintain a rolling three months of backups which are encrypted using AES-256.

Please [click here](#) for a list of sub-processors.

How data is kept secure

We employ appropriate technical and organisational security measures for the types of data we store. Our managed hosting provider, UKFast, is ISO 27001 & ISO 9001 accredited and ranks amongst the very best in the industry. They offer physical security such as 24/7 security staff, extensive CCTV covering the building and each aisle, intruder alarms, proximity card readers and perimeter prison fencing.

We apply the latest patches to our servers keeping your data safe and secure with multiple levels of password protection - the servers themselves and the database each are password protected. Additionally the servers are behind a redundant pair of Cisco hardware firewalls. Annual vulnerability scanning is provided by UKFast.

Subject access requests from end-users

As data processors, we are obliged to pass on to the school any subject access request by an end-user and not respond directly to the end-user. An end-user could be a parent, student, teacher or administrator of the system. We will assist the school in responding to any subject access request.

What happens if you stop using the system

This section takes effect as of 25th May 2018

While it's rare for a school to stop using SchoolCloud Parents Evening, we only retain personal data for as long as necessary. You can retrieve a copy of all personal data using the export features within the administration panel while the system remains active during your trial period or paid licence period. We delete personal data 30 days following termination of your licence or after six months of inactivity if you have a trial system. We terminate the licence 60 days after the renewal date if no payment has been received for the renewal.

Features to help comply with GDPR

Syncing data with your school management system

Whenever you choose to sync data from your school management information system (MIS), we add new data, update existing records with the latest information from your MIS, and delete records which are no longer relevant or no longer appear in your MIS. Most MIS suppliers are implementing controls to restrict sharing personal data via their API's where you, as the data controller, do not wish it to be shared with third parties. Please contact your MIS supplier directly with any questions.

Exports for data portability

It's possible to export data added to SchoolCloud Parents Evening to spreadsheets to satisfy data portability. You can export all bookings for a particular parents' evening or event from the Appointments or Bookings pages retrospectively. This process can be repeated for each parents' evening & event for which you wish to export data for. It's also possible to export a list of parent details, including links to students.

Data held about Schools

We act as **data controllers** for any data we collect about customers in order to provide SchoolCloud Parents Evening service and support to your school. Customer personal data includes, but is not limited to: technical contact details, finance contact details, phone call details, and the content & attachments of any emails sent to us.

Where data is held

Data is stored on production systems hosted by UKFast and in backups hosted by AWS. Please [click here](#) for a list of sub-processors.

Transfers of customer personal data

While we're based in the UK, we use suppliers outside the EEA to run our business. Customer personal data (though not end-users such as parents, students or teachers) may be transferred outside the EEA to suppliers who demonstrate sufficient safeguards on data using one of the following legal mechanisms: the

EU-U.S. Privacy Shield, or the Standard Contractual Clauses.

Emails sent to us are processed by Help Scout, who host their data with Amazon Web Services in their US data centres. Help Scout Inc. complies with the EU-U.S. Privacy Shield Framework. Help Scout Inc. has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles.

School Library Systems

Please find link to school Library Systems Privacy Policy

<http://www.schoollibrary.co.uk/docs/PrivacyDocumentGDPR1.pdf>

Other platforms we use that may ask / store or use pupil information.

Company	Link to Privacy Policy	Department Using
Isaac Computer Science	https://isaacomputerscience.org/privacy	Computer Science
eRevision.uk	https://erevision.uk/welcome/privacyPolicy	Computer Science
Repl.it	https://repl.it/site/privacy	Computer Science
Social Care Institute for Excellence	https://www.scie.org.uk/about/privacy.asp	Health & Social Care
Revision World	https://revisionworld.com/content/privacy	Law
SENECA Learning	https://senecalearning.com/en-GB/privacy	All
Quizlet	https://quizlet.com/privacy	All
Cool Geography	https://www.coolgeography.co.uk/privacy.php	Geography
BBC Bitesize	https://www.bbc.co.uk/usingthebbc/privacy	All
Learndojo	https://learndojo.org/privacy-policy/	Psychology
Linguascope	https://www.linguascope.com/info/privacypolicy.htm	French
Wand Education	https://wand.education/privacy-policy-2/	Exams
Abracadabra.net	http://www.schoollibrary.co.uk/docs/PrivacyDocumentGDPR1.pdf	Library
School Cloud	https://www.schoolcloud.co.uk/privacy-notice.asp	Office / I.T. Parents Evening
SNAP Assessment	https://www.hoddereducation.co.uk/privacynotice	Special Educational Needs Department
GL Assessment	https://www.gl-assessment.co.uk/support/privacy-policy/	Exams
VeriCool	https://www.vericool.co.uk/Data Protection and Privacy.php	Canteen
Maths Watch	https://vle.mathswatch.co.uk/privacy-policy/	Maths
Century-Tech Limited	https://www.century.tech/wp-content/uploads/2020/03/CENTURY-Tech-Privacy-Policy.pdf	English, maths and science