Appendix A - 3rd Parties

ALPS	ALPS: The School may send information about learners to a third party organisation called ALPS for the provision of software products delivered over the internet.The information required by ALPS includes the pupil first name, surname, gender, DOB, Ethnicity, disaadvantaged, exam results. ALPS's services are valuable in helping educational organisations to monitor and improve the quality of education they provide by allowing them to analyse student and subject performance in great depth.
AMI Education	AMI: This software is used to provide our cashless catering system. AMI Education Solutions software products hold Personal Data sourced from the school MIS (or created manually by the school), the data is used to verify the identity of an individual at the point of service delivery via computer terminals, EPOS terminals and Coin & Note revaluation units. The data is stored on school servers and AMI only have access to this data in order to provide support for the system when authorised by the school. The categories of data subject to whom the Personal Data relates to are Pupils, Students, Employees and any authorised visitors that require access to related services. The types of Personal Data to be processed includes: - Surname, Legal Surname, Forename, Legal Forename, Registration Group, Year, Tutor, Date of Birth, Gender, Free Meal Eligibility, UPN, Admission Number, MISID, Photograph, Biometric template*, Dietary needs, Transactional data Purchases, credits, and refunds. These are related to personal records using a system generated identifier. We may share this information with our online payment provider Tucasi (details listed under Tucasi). *Biometric Data will only be stored with consent. The Biometric database is encrypted using AES256 - an industry standard and highly secure technology. All communications between applications and the database are also encrypted using AES256. Each school has its own secret unique group of AES256 encryption keys, which means that the database and any backup of its contents can only be accessed on licensed hardware, and the encrypted data is only available to the registered licensee. AES256 is the same encryption technology that is used in Microsoft's BitLocker disk drive encryption, and is certified by the National Security Agency of America to be used to protect Top Secret information.
Awarding Bodies	AQA, Pearsons, WJEC/Eduqas, OCR, Cambridge Assessment Admissions Testing: These awarding bodies are used to provide national examinations at various levels including GCSE, Entry Level, A Level.
BROMCOM	BROMCOM: Bromcom is our main Management Information System that is used to store all student data in order for us to fulfill our statutory obligations in the provision of education for your child. Beyond the delivery of statutory data to the DFE through mechanisms such as the school and workforce census, Bromcom does not automatically share your data with anyone else and does not grant third parties access. Any third parties will need to liaise with the school to be given permission to access your data and permission will only be granted if it is needed to improve the quality of education and care of your child.The Bromcom database is securely stored and access is managed through our provider who is ISO 9001, 14001 and 27001 accredited and PCI DSS compliant. With strict information security protocols, your systems are protected around the clock in Bromcom's secure data centres with access to technical support 24/7/365.
CPOMS	CPOMS: Safeguarding recording information. Due to the sensitive nature of safeguarding requirements it is necessary for us to be able to share all data we hold in our MIS alongside specification information on any safeguarding incidents. CPOMS is registered with the UK Information Commissioner's Office both as a Data Processor for customers' data and as a Data Controller for their own company's data. They are also accredited for both ISO 27001 and UK Government 'Cyber Essentials' which are reviewed each year. They also subject their systems and networks to regular independent penetration testing to ensure the security of our schools' data.
Evolve	Learning outside the classroom, school trips: The School may send information about learners to a third party organisation called EVOLVE for the risk assessment and storage of information regarding the provision of learning outside the classroom.The information required by EVOLVE includes the pupil first name, surname, gender, DOB, disaadvantaged, medical details, dietary requirements and contact details of parents/carers. Evolve's services are valuable in helping educational organisations to risk assess and safeguard our students when learning outside of the school. This information may be shared with the Local Authority when additional risk assessment is required for residential trips.

GL Assessment	GL Assessment: As part of our assessment programme we use several sets of student data to monitor your child's progress and inform our teaching. One of the tools we use is the CAT4 Test/ Progress Test Series from GL Assessment to give us an acute understanding of a student's potential. This data is considered alongside any other assessments made throughout the year, formal or informal, to inform our teaching
Google	Google: Google provides email, document storage and online classroom facilities to enhance the quality of teaching and learning. Google will implement and maintain technical and organizational measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. Security Measures include measures to encrypt personal data; to help ensure ongoing confidentiality, integrity, availability and resilience of Google's systems and services. Google may transfer data outside of the EU but is fully compliant under GDPR regulations by the signing of a model clauses contract approved by the European Commission.
Groupcall	Groupcall - Groupcall is used to securely transfer data from our MIS to our 3rd parties using Xporter on Demand (XoD). XoD will proactively cache a limited set of data based on the data areas we authorised (see each 3rd party for details of the data that is shared) . This cache is AES encrypted with a unique key before leaving the school. Expired cache data is securely erased automatically after 30 days, or sooner by request. Caches are refreshed daily, or on demand if required.
Inspire	Inspire: teacher cover suppliers. Cover supervisors who are covering a lesson for an absent member of staff have limited access to data on the class they are supervising. This may include student names, DOB, assessment data, SEN needs. None of this information is taken off site or stored by Inspire. It is only available to the supervisor at the time of their deployment.
MintedBox	MINTclass is a powerful suite of products for schools which includes a seating planner that enables teaching staff to automatically create and manage their classroom seating plans. Information, including first name, surname, gender, ethnicity, SEN code, grades and other factors such as pupil premium, about each student is displayed in an easy to use manner. Information is extracted from the school Management Information System (MIS) using Groupcall's industry leading and secure Xporter software. The data is securely uploaded to MINTclass using industry standard SSL encryption.
PiXL	PIXL: Pixl provides classroom strategies and resources to improve best practice and to raise standards of teaching and learning for students The types of student personal data processed will usually include names, login information, school email addresses. For some applications, year, class, and attainment data are processed. Best practice security techniques, such as anonymisation and encryption, are applied to transfers of personal data between the Member School and PiXL, between all data servers and between servers and end point devices.
PRIME	Prime: Health and Safety incident recording system. This system is used to record incidents where an accident has happened on the school premises and has involved a fracture or anything where a hospital visit straight from school has been necessary. The data recorded will be name, gender, DOB and details of the accident. This is a requirement of the Health & Safety Executive.
Renaissance Learning - Accelerated Reader	Acclerated Reader: This is a literacy programme to help students advance their literacy skills. The online system stores information including name, DOB, gender, main language,Pupil Premium, Free School Meals, Assessment data on reading tests. Renaisance Learning stores the information in the US and is certified under the EU-US Privacy Shield.
School Cloud Systems	Parents Evening Booking System: This online system is used by parents to book appointments to see students teachers. The system contains information on students including name, DOB and timetabled classes and contact information for parents/carers. They employ appropriate technical and organisational security measures for the types of data they store. Their managed hosting provider, UKFast, is ISO 27001 & ISO 9001 accredited and ranks amongst the very best in the industry.
SchoolComms	Schoolcomms: This software is used for home school communications. The information required by Schoolcomms includes forename, surname, gender, DOB, assessment data, behaviour, achievement, attendance, timetable information and contacts information. Schoolcomms have introduced appropriate technical and organisational measures to protect the confidentiality, integrity and availability of your personal information during storage, processing and transit. They are a Level 2 PCI-DSS certified organisation and operate an ISO27001 compliant security programme.

SISRA	SISRA Limited: The School may send information about learners to a third party organisation called SISRA Limited for the provision of software products delivered over the internet.The information required by SISRA Limited includes the pupil first name, surname, gender, ethnicity, SEN code and other factors such as "Free School Meals", "Gifted & Talented" and "Children in Care". SISRA's services are valuable in helping educational organisations to monitor and improve the quality of education they provide by allowing them to analyse student, class and subject performance in great depth. In addition to the above, the school may request the services of one or more of SISRA's Data Consultants to visit the school. The purpose of the visit may require authorised access to the school's management information system (MIS), which could mean access to sensitive personal data. The school will fully supervise any access while the SISRA Data Consultant is on the premises and remain responsible for any data processing that the SISRA Data Consultant might perform. Data Protection Officer, SISRA Limited, Egerton House, 2 Tower Road, Birkenhead, Merseyside. CH41 1FN.
Sodexo	Sodexo: Sodexo are our catering company. In order to provide meals to our students Sodexo staff have access to our cashless catering system and associated data (see AMI Education listed above). This data is only accessible when they are on the school site. Sodexo share dietary requirements with their nutritionist so they can meet the requirements of our students. If payment is made to Sodexo by cheque then copies of these cheques are kept by Sodexo for a period of 5 years. Daily transaction records, including online payments are also kept by Sodexo for 5 years.
Survey Monkey	Survey Monkey: Survey Monkey is used to send surveys to staff, students and visitors. While we don't share your information with Survey Monkey directly some of the question responses may contain personal information. When this data is entered into a survey response it will be stored by Survey Monkey once the response is submitted. Survey Monkey will also record additional information such as Cookies and IP addresses of their visitors to ensure the surveys function as intended. SurveyMonkey's information systems and technical infrastructure are hosted within world-class, SOC 2 accredited data centers. Physical security controls at their data centers include 24x7 monitoring, cameras, visitor logs, entry requirements, and dedicated cages for SurveyMonkey hardware. Data is held on US servers and Survey Monkey contractually comply with the EU-US Privacy Shield to allow transfer of the data outside the EU.
Team Satchel (Teachercentric Ltd)	Show My Homework: This software is used to record and share with parents and students homework set by classroom teachers improving standards of teaching and learning for students The types of student personal data processed will usually include names, school email addresses, timetable information and parental names . Satchel are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, they have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information they collect online.
Tempest Photography	School official photographers: This company carries out official school photos. The data that is shared with Tempest in order to identify the students when uploading photos onto our school MIS is the stutents tutor group and admission number. At Tempest, they have a secure portal, using the latest 256-bit data encryption, specifically for these purposes. They provide schools with instructions on how to provide any information that has to be shared via their secure portal in a compliant manner.
Tucasi	Tucasi - Schools Cash Office helps the school to manage payments coming into the school and is linked with SCOPay the online payment system used by parents. Tucasi stores Names, DOB, Address, Pupil Premium and contact details. Tucasi also stores the balance for the cashless catering system and a record of items that have been purchased. In order to provide these links Tucasi may share some information to the cashless catering system (see AMI education). It is important to understand that Tucasi Limited does not take or store your financial data. This website allows users to select items that need to be paid for, but payment processing is handled by WorldPay based on information parents enter when making a payment.
Twitter	Twitter: The school uses a number of Twitter accounts to share information, celebrate achievements and blog about trips and events. The information posted on Twitter may include first names and, where consent is given, photographs. The information posted on Twitter is public and as such may be copied and shared outside of our control.

Vericool	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. No third party data is held by Vericool Ltd. All data for their 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. For purposes of support Vericool engineers may require authorised access to the onsite Vericool database this access is supervised by school staff. On very rare occasions and with the explicit permission of the school Vericool 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. All data is hard deleted as soon as it is finished with and it is their policy to physically destroy the hard disk once a year. They do not share any information with any third parties and conduct no marketing or data analysis using it.
WIX	Wix: The school uses Wix to build and host our website. All information published on our website is publicly available and may be copied and shared outside of our control. We may publish firstnames, and where consent is given, photographs. When you visit Wix they may record information such as Cookies and IP addresses. Wix.com is certified under the EU-US Privacy Shield Framework and the Swiss-US privacy Shield Framework as set forth by the U.S. Department of Commerce, regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, and therefore adheres to the Privacy Shield Principles.