WISHFORD EDUCATION

PRIVACY NOTICE & DATA PROTECTION POLICY

This policy applies to all settings within the Wishford Education Group.

Date of Policy	**September 2024**
Member of staff responsible	**Mr Paul Easterbrook**
Role	**Director of Education & Compliance**

Last Review	**Significant changes**
	Change of name to Wishford Education.

1. Policy Scope

a. This policy relates to all current, past and prospective pupils, parents/carers (**External Privacy Notice**) and staff (**Staff Privacy Notice**), including contractors/volunteers across the entire Wishford Education Group.
b. The aim of this policy is to prevent any harm because of a data breach.
c. It applies in addition to The Group's terms and conditions and any other information The Group may provide about a particular use of personal data e.g. The Group's IT Acceptable Use Policy.
d. It is in accordance with GDPR and The Data Protection Act 2018 ('the Act'),
e. The Group has notified the Information Commissioner's Office of its processing activities. The Group's ICO registration number is ZA560394 and its registered address is 25-27 High St, Corsham, Wiltshire SN13 0ES.
f. The Group has appointed Paul Easterbrook as Data Protection Officer ("DPO") who will ensure that all personal data is processed in compliance with this policy and the Act.

Personal data must be recorded, processed, transferred and made available according to the current data protection legislation. Each setting must ensure that:

1. It follows this Group Data Protection Policy which records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed).
2. It ensures all stakeholders are aware of this policy and have easy access to it (e.g. via the setting website).
3. It follows any additional guidance from the Group Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
4. It has an up to date 'record of data processing' and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it.
5. Personal data is accurate and up to date (where this is necessary for the purpose it is processed for). And systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
6. Where special category data is processed, an additional lawful basis will have also been recorded.
7. It will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary and within the stated timeframes.
8. Procedures are in place to deal with the individual rights of the data subject, e.g. processing a Subject Access Request (SAR).
9. It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
10. It understands how to share data lawfully and safely with other relevant data controllers.
11. It reports any relevant breaches to the Information Commissioner (via the DPO: data.protection@wishford.co.uk) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law.
12. Ensures all staff receive data protection training relevant to their role at induction and appropriate refresher training thereafter, with a particular focus on adherence to this policy.

2. Principles and Definitions

The law changed on 25 May 2018 with the implementation of the General Data Protection Regulation (GDPR) – an EU Regulation that is directly effective in the UK, regardless of Brexit status – and a new Data Protection Act 2018 (DPA 2018) was also passed to deal with certain issues left for national law. The DPA 2018 included specific provisions of relevance to educational settings: in particular, in the context of our safeguarding obligations, and regarding the right of access to personal data.

The Principles

The GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for specific and explicit purposes and only used for the purposes it was collected for;
3. Relevant and limited to what is necessary for the purposes it is processed;
4. Accurate and kept up to date;
5. Kept for no longer than is necessary for the purposes for which it is processed; and
6. Processed in a manner that ensures appropriate security of the personal data.

The GDPR's broader 'accountability' principle also requires that the group not only processes personal data in a fair and legal manner but that we are also able to demonstrate that our processing is lawful. This involves, among other things:

- keeping records of our data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how we use personal data (including via formal risk assessment documents called Data Protection Impact Assessments); and
- generally having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notice(s) were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

Definitions
Key data protection terms used in this data protection policy are:

- **Data controller** – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. For example, a setting (including its management team) is a controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.
- **Data processor** – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.
- **Personal data:** any information relating to a living individual (a data subject) by which that individual may be identified by the controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the College's, or any person's, intentions towards that individual.
- **Personal data breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- **Processing** – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.
- **Special categories of personal data** – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

3. External Privacy Notice (Pupils & Parents)

a. The scope of this privacy notice

i. This notice is for Wishford Education (Group) Ltd (The Group), the data controller for the purposes of this Privacy Notice under the Data Protection Law and relevant policies (General Data Protection Regulation [EU 2016/679] and the UK Data Protection Act 2018.) Wishford Education (Group) Ltd is a company, registered in England with registration number 8982719.
ii. This notice is intended to provide information about how The Group will use (or "process") the personal data individuals who do not work for, or act on behalf of The Group, including: its current, past and prospective pupils; and their parents, carers or guardians (referred to in this notice as "parents").
iii. This notice is provided because Data Protection Law gives individuals rights to understand how their data is used. Parents and pupils are all encouraged to read this Privacy Notice and understand The Group's obligations to its entire community.
iv. This notice applies alongside any other information The Group may provide about a particular use of personal data.
v. This notice also applies in addition to The Group's other relevant terms and conditions and policies, including: The contract between The Group and the parents of pupils as set out in The Group's Terms of Business; The Group's IT: Acceptable Use policy; and The Group's Safeguarding and Health and Safety policies.
vi. Any individual who works for, or acts on behalf of, The Group (including staff, volunteers, governors and service providers) should be aware of and comply with this notice when dealing with your data.

b. Oversight

The Group has appointed Paul Easterbrook as the Data Protection Officer email: data.protection@wishford.co.uk; Tel: +44 (0)1249 713908) who will deal with all your requests and enquiries concerning The Group's uses of your personal data (see section on Your Rights below) and endeavour to ensure that all personal data is processed in compliance with this policy and Data Protection Law.

c. Reasons for processing personal data

In order to carry out its ordinary duties to pupils and parents, The Group needs to process a wide range of personal data about individuals (including current, past and prospective pupils or parents) as part of its daily operation. The Group will need to carry out some of this activity in order to fulfil its legal rights, duties or obligations, or otherwise as necessary to fulfil contractual obligations. The Group expects that the following uses will fall within those categories:

i. For the purposes of the admissions of pupils to The Group (and to confirm the identity of prospective pupils and their parents);
ii. To provide education services, including musical education, physical training or spiritual development and extra-curricular activities to pupils, and monitoring pupils' progress and educational needs;
iii. Maintaining relationships with alumni and The Group community, including direct marketing, event notification or fundraising activity, including by sending updates and newsletters, by email and by post;
iv. To enable relevant authorities to monitor The Group's performance and to intervene or assist with incidents as appropriate;
v. To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil attended or where it is proposed they attend; and to provide references to potential employers of past pupils;
vi. To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of The Group;
vii. To safeguard pupils' welfare and provide appropriate pastoral care;
viii. To monitor (as appropriate) use of The Group's IT and communications systems in accordance with The Group's IT: Acceptable Use policy;

ix. To make use of photographic images of pupils in setting publications, on The Group's websites and (where appropriate) on The Group's social media channels in accordance with The Group's IT Acceptable Use policy;
x. For security purposes;
xi. To carry out or cooperate with any setting or external complaints, disciplinary or investigation process; and
xii. Where otherwise reasonably necessary for The Group's purposes, including to obtain appropriate professional advice and insurance for The Group.
xiii. To share limited personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with The Group community;

In addition, The Group will on occasion need to process special category personal data (concerning health, ethnicity, religion, biometrics or sexual life) or criminal records information (such as when carrying out DBS checks) in accordance with rights or duties imposed on it by law, including as regards safeguarding and employment, or from time to time by explicit consent where required. These reasons will include:

xiv. To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency, incident or accident, including by disclosing details of an individual's medical condition or other relevant information where it is in the individual's interests to do so: for example for medical advice, for social protection, safeguarding, and cooperation with police or social services, for insurance purposes or to caterers or organisers of setting trips who need to be made aware of dietary or medical needs;
xv. To provide educational services in the context of any special educational needs of a pupil;
xvi. To provide spiritual education in the context of any religious beliefs;
xvii. As part of any setting or external complaints, disciplinary or investigation process that involves such data, for example if there are SEN, health or safeguarding elements; or
xviii. For legal and regulatory purposes (for example child protection, diversity monitoring and health and safety) and to comply with The Group's legal obligations and duties of care).

d. Types of data

This will include by way of example:

i. names, addresses, telephone numbers, e-mail addresses and other contact details;
ii. car details (about those who use our car parking facilities);
iii. bank details and other financial information, e.g. about parents who pay fees to The Group; past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks;
iv. where appropriate, information about individuals' health and welfare, and contact details for their next of kin;
v. references given or received by The Group about pupils, and relevant information provided by previous educational establishments and/or other professionals or organisations working with pupils;
vi. correspondence with and concerning pupils and parents past and present; and
vii. images of pupils (and occasionally other individuals) engaging in setting activities, and images captured by The Group's CCTV system;

e. Data collection

Generally, The Group receives personal data from the individual directly (including, in the case of pupils, from their parents). This may be via a form, or simply in the ordinary course of interaction or communication (such as email or written assessments). However, in some cases personal data will be supplied by third parties (for example another setting, or other professionals or authorities working with that individual); or collected from publicly available resources.

f. Data management

i. Occasionally, The Group will need to share personal information relating to its community with third parties, such as: professional advisers (e.g. lawyers, insurers, PR advisers and accountants); government authorities (e.g. DfE, police or the local authority); and appropriate regulatory bodies

e.g. Teaching Regulation Agency, the Independent Schools Inspectorate, OFSTED or the Information Commissioner.

ii. For the most part, personal data collected by The Group will remain within The Group, and will be processed by appropriate individuals only in accordance with access protocols (i.e. on a 'need to know' basis). Particularly strict rules of access apply in the context of: medical records held and accessed only by appropriate staff, or otherwise in accordance with express consent; and pastoral or safeguarding files. However, a certain amount of any SEN pupil's relevant information will need to be provided to staff more widely in the context of providing the necessary care and education that the pupil requires.

iii. Staff, pupils and parents are reminded that The Group is under duties imposed by law and statutory guidance (including Keeping Children Safe in Education) to record or report incidents and concerns that arise or are reported to it, in some cases regardless of whether they are proven, if they meet a certain threshold of seriousness in their nature or regularity. This is likely to include file notes on personnel or safeguarding files, and in some cases referrals to relevant authorities such as the LADO or police. For further information about this, please view The Safeguarding Policy.

iv. In all cases of data management, staff across the group have been made aware of the following minimum standards as part of their training on this policy:

- All staff must read this policy and the IT: Acceptable Use policy and sign the Acceptable Use agreement.
- Personal data is not printed into a hard copy unless absolutely necessary.
- Hard copies which include personal data should not leave the setting site unless absolutely necessary and, in all cases where it is necessary, the data should remain under close supervision and not taken into public spaces.
- Electronic data should be stored on secure systems which are encrypted and password protected.
- Devices used to process data must be password protected and have up to date virus and malware checking software installed.
- Devices and accounts should be logged off/locked after use.
- Only setting devices should be used to process personal data. If personal data has to be temporarily downloaded onto a personal device, it should be deleted at the earliest possible convenience.
- Group emails/correspondence should go through the setting office and all staff must remain vigilant and ensure that personal data is not shared with others via setting publications.
- Staff must be able to recognise a data breach and know the reporting process.

v. Some of The Group's processing activity is carried out on its behalf by third parties, such as IT systems, web developers or cloud storage providers. This is always in accordance with Data Protection Law and therefore subject to contractual assurances that personal data will be kept securely and only in accordance with The Group's specific directions.

e. Retaining Data

i. The Group will retain personal data securely and only in line with how long it is necessary to keep for a legitimate and lawful reason.

ii. Typically, the legal recommendation for how long to keep ordinary pupil personnel files is up to 7 years following departure from The Group. However, incident reports and safeguarding files may need to be kept longer, in accordance with any specific legal requirements.

iii. If you have any specific queries about our retention of data, or wish to request that personal data that you no longer believe to be relevant is considered for erasure, please contact The Group's data protection officer, please bear in mind that The Group will often have lawful and necessary reasons to hold on to some personal data even following such request.

iv. A limited and reasonable amount of information will be kept for archiving purposes, for example, a list of archived contact details, and even where you have requested we no longer keep in touch with you, we will need to keep a record of the fact in order to fulfil your wishes (called a "suppression record").

f. Your rights

The rights under Data Protection Law belong to the individual to whom the data relates. The Group will often rely on parental authority or notice for the necessary ways it processes personal data relating to pupils – for example, under the parent contract, or via a form. Parents and pupils should be aware that

this is not necessarily the same as The Group relying on strict consent. Where consent is required, it may in some cases be necessary or appropriate – given the nature of the processing in question, and the pupil's age and understanding – to seek the pupil's consent. Parents should be aware that in such situations they may not be consulted, depending on the interests of the child, the parents' rights at law or under their contract, and the specific circumstances.

In general, The Group will assume that pupils' consent is not required for ordinary disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare. That is unless, in The Group's opinion, there is a good reason to do otherwise. However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, The Group may be under an obligation to maintain confidentiality unless, in The Group's opinion, there is a good reason to do otherwise; for example, where The Group believes disclosure will be in the best interests of the pupil or other pupils, or if required by law. Pupils are required to respect the personal data and privacy of others, and to comply with The Group's policies, e.g. ICT policy and The Group rules. Staff are under professional duties to do the same covered under the relevant staff policy.

Nevertheless, in all cases, pupils and parents should take note of the following guidance:

i. Individuals have various rights under Data Protection Law to access and understand personal data about them held by The Group, and in some cases ask for it to be erased or amended or have it transferred to others, or for The Group to stop processing it, albeit subject to certain exemptions and limitations. Any individual wishing to access or amend their personal data, or wishing it to be transferred to another person or organisation, or who has some other objection to how their personal data is used, should put their request in writing to The Group's Data Protection Officer.
ii. The Group will endeavour to respond to any such written requests as soon as is reasonably practicable and in any event within statutory time-limits (which is one month in the case of requests for access to information).
iii. The Group will be better able to respond quickly to smaller, targeted requests for information. If the request for information is manifestly excessive or similar to previous requests, The Group may ask you to reconsider, or require a proportionate fee (but only where Data Protection Law allows it).
iv. You should be aware that the right of access is limited to your own personal data, and certain data is exempt from the right of access. This will include information which identifies other individuals (and parents need to be aware this may include their own children, in certain limited situations – please see further below), or information which is subject to legal privilege (for example legal advice given to or sought by The Group, or documents prepared in connection with a legal action).
v. The Group is also not required to disclose any pupil examination scripts (or other information consisting solely of pupil test answers), provide examination or other test marks ahead of any ordinary publication, nor share any confidential reference given by The Group itself for the purposes of the education, training or employment of any individual, referred to as the "right to be forgotten".
vi. The Group will sometimes have compelling reasons to refuse specific requests to amend, delete or stop processing your (or your child's) personal data: for example, a legal requirement, or where it falls within a legitimate interest identified in this Privacy Notice. All such requests will be considered on their own merits.
vii. Pupils can make subject access requests for their own personal data, provided that, in the reasonable opinion of The Group, they have sufficient maturity to understand the request they are making.
viii. A pupil of any age may ask a parent or other representative to make a subject access request on his/her behalf. Indeed, while a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils, the law still considers the information in question to be the child's: for older pupils, the parent making the request may need to evidence their child's authority for the specific request.
ix. It should be clearly understood that the rules on subject access are not the sole basis on which information requests are handled. Parents may not have a statutory right to information, but they and others will often have a legitimate interest or expectation in receiving certain information about pupils without their consent. The Group may consider there are lawful grounds for sharing with or without reference to that pupil. Parents will in general receive educational and pastoral updates about their children, in accordance with the Parent Contract and prevailing legislation.

x. Where parents are separated, The Group will in most cases aim to provide the same information to each person with parental responsibility, but may need to factor in all the circumstances including the express wishes of the child. All information requests from, on behalf of, or concerning pupils – whether made under subject access or simply as an incidental request – will therefore be considered on a case by case basis.

xi. Where The Group is relying on consent as a means to process personal data, e.g. the use of images, any person may withdraw this consent at any time (subject to similar age considerations as above). The Group may process such data without consent for a legitimate lawful reason.

xii. GDPR includes a number if rights which we as a Group recognise and consider for each individual case:

- The right to be informed – data will be kept by the setting and all parties kept informed as to how the data is used in a way that is easy to access, read and understand
- The right of access – individuals have the right to obtain conformation of how their data is being processed and used. A copy of all the information is provided free if charge within ine calendar month of a request.
- The right to rectification – Inaccurate data can be rectified and if a request is made a response is given within one calendar month
- The right to erasure- The request is responded to within one calendar month buyt there might be circumstances where this right does not apply
- The right to restrict processing- individuals can request their data is restricted in its use where personal data is inaccurate or an individual wants to limit how an organisation uses their data. Again the one calendar month response time applies.
- The right to data portability- individuals can obtain and reuse their personal data for their own purposes across different services
- The right to object -individuals have the right to object to processing their personal data based on legitimate interests to opt out. This includes the purpose of direct marketing, profiling and scientific/historic research and statistics.
- The right to withdraw consent – where consent is relied on. This does not mean previously processed data reliant on consent becomes unlawful or must be necessarily rectified but the withdrawal will be respected
- Rights in relation to automated decision making and profiling – only carry out automated decision making or automated processing of personal data, including profiling where this tyoe of decision making is for a contract, authorised by Union or Member state law or based on the individual's consent.

g. Queries and complaints

Any comments or queries on this policy should be directed to The Group's data protection officer directly. If an individual believes that The Group has not complied with this policy or acted otherwise than in accordance with Data Protection Law, they should utilise The Group complaints procedure and should also notify The Groups data protection officer. You can also make a referral to or lodge a complaint with the Information Commissioner's Office (ICO), although the ICO recommends that steps are taken to resolve the matter with The Group before involving the regulator.

4. Staff Privacy Notice

In the course of your work undertaken for Wishford Education (Group) Ltd. (The Group), we will collect, use and hold ("process") personal data relating to you as a member of our staff or wider setting team, regardless of your employment status. This makes The Group a data controller of your personal information, and this Privacy Notice sets out how we will use that information and what your rights are.

a. Who this document applies to

i. Academic and other staff, contractors, visiting music teachers and other peripatetic workers, casual workers, temps, and volunteers who may be employed or engaged by The Group to work for it in any capacity, as well as prospective applicants for roles. It also applies to directors.
ii. Please note that any references to "employment", "staff" etc. in this Notice are not intended to imply or confer any employment rights on you if you are a contractor, non-employed worker, or job applicant, even if the Notice is relevant to how we process your personal data.
iii. This notice is not aimed at pupils, or parents of pupils (whether current, past or prospective) or other members of the public.

b. About this document

i. This Staff Privacy Notice explains how The Group collects, uses and shares (or "processes") personal data of staff, and your rights in relation to the personal data we hold.
ii. This Privacy Notice also applies in addition to The Group's other relevant terms and conditions and policies that may (depending on your role and status) apply to you, including any contract between The Group and its staff, such as the terms and conditions of employment, and any applicable staff handbook/code of conduct and relevant policies such as IT: Acceptable Use, Safeguarding and all pastoral & H&S policies.
iii. Please note that your contract with or engagement by The Group, including any document or policy forming a part of your contractual obligations to The Group, may in particular be relevant to (and supplement the information in) this Staff Privacy Notice, to the extent that it will contain details of obligations or rights of The Group under contract with you which may require the use of your personal data. However, this Staff Privacy Notice is the primary document in terms of how we notify you about the use of your personal data by The Group.
iv. This Staff Privacy Notice also applies alongside any other information The Group may provide about particular uses of personal data, for example when collecting data via an online or paper form.

c. How we collect your information

i. from the information you provide to us before making a job application, for example when you come for an interview;
ii. when you submit a formal application to work for us, and provide your personal data in application forms and covering letters, etc.; and
iii. from third parties, for example the Disclosure and Barring Service (DBS) and referees (including your previous or current employers or setting), or (if you are a contractor or a substitute) your own employer or agent, in order to verify details about you and/or your application to work for us.
iv. when you provide or update your contact details;
v. when you or another member of staff completes paperwork regarding your performance appraisals;
vi. in the course of fulfilling your employment (or equivalent) duties more generally, including by filling reports, note taking, or sending emails on setting systems;
vii. in various other ways as you interact with us during your time as a member of staff, and afterwards, where relevant, for the various purposes set out below.

d. The types of information we collect

We may collect the following types of personal data about you (and your family members and 'next of kin', where relevant):

i. contact and communications information, including:
   - your contact details (including email address(es), telephone numbers and postal address(es);
   - contact details (through various means, as above) for your family members and 'next of kin', in which case you confirm that you have the right to pass this information to us for use by us in accordance with this Privacy Notice;
   - records of communications and interactions we have had with you;

ii. biographical, educational and social information, including:
   - your name, title, gender, nationality and date of birth;
   - your image and likeness, including as captured in photographs taken for work purposes;
   - details of your education and references from your institutions of study;
   - lifestyle information and social circumstances;
   - your interests and extra-curricular activities;

iii. financial information, including:
   - your bank account number(s), name(s) and sort code(s) (used for paying your salary or invoices and processing other payments);
   - your tax status (including residence status);
   - information related to pensions, national insurance, or employee benefit schemes;

iv. work related information, including:
   - details of your work history and references from your previous employer(s);
   - your personal data captured in the work product(s), notes and correspondence you create while employed by or otherwise engaged to work for The Group;
   - details of your professional activities and interests;
   - your involvement with and membership of sector bodies and professional associations;
   - information about your employment and professional life after leaving The Group, where relevant (for example, where you have asked us to keep in touch with you);

v. and any other information relevant to your employment or other engagement to work for The Group.

Where this is necessary for your employment or other engagement to work for us, we may also collect special categories of data, and information about criminal convictions and offences, including:

vi. information revealing your racial or ethnic origin;
vii. trade union membership, where applicable;
viii. information concerning your health and medical conditions (for example, where required to monitor and record sickness absences, dietary needs, or to make reasonable adjustments to your working conditions or environment);
ix. biometric information, for example where necessary for setting security systems;
x. information concerning your sexual life or orientation (for example, in the course of investigating complaints made by you or others, for example concerning discrimination); and
xi. information about certain criminal convictions (for example, where this is necessary for due diligence purposes, or compliance with our legal and regulatory obligations);
xii. However, this will only be undertaken where and to the extent it is necessary for a lawful purpose in connection with your employment or other engagement to work for The Group.

e. Processing data

A candidate, employee, contractor or volunteer will have their personal data processed by The Group to facilitate the fulfilment of all contractual and legal obligations. Examples of activities which might include data processing include:

i. administering job applications and, where relevant, offering a role;
ii. carrying out due diligence checks on candidates, whether during the application process for a role or during initial engagement, including by checking references in relation to education and employment history;
iii. fulfilling the terms of the contract of employment (or other agreement);
iv. paying income and benefits;
v. monitoring attendance and performance;
vi. promoting The Group to prospective parents and others, including by publishing material created by individuals working for or on behalf of The Group;
vii. carrying out disciplinary procedures, including conducting investigations where required;

viii. updating terms and conditions of employment or engagement and/or pension arrangements;
ix. managing internal record-keeping, including the management of any staff feedback or complaints and incident reporting; and
x. for any other reason or purpose set out in employment/engagement contracts/agreements.

Depending on role and status, we process special categories of personal data (such as data concerning health, religious beliefs, racial or ethnic origin, sexual orientation or union membership) or criminal convictions and allegations for the reasons set out below. We will process this data on the basis that such processing is necessary to carry out obligations and exercise rights (for all parties) in relation to employment or engagement. In particular, we may process the following types of special category personal data for the following reasons:

xi. your physical or mental health or condition(s) in order to record sick leave and take decisions about your fitness for work, or (in emergencies) act on any medical needs you may have;
xii. categories of your personal data which are relevant to investigating complaints made by you or others, for example concerning discrimination, bullying or harassment;
xiii. data about any criminal convictions or offences committed by you, for example when conducting criminal background checks with the DBS, or where it is necessary to record or report an allegation (including to police or other authorities, with or without reference to you);

We will process special categories of personal data for lawful reasons only, including because:

xiv. you have given us your explicit consent to do so, in circumstances where consent is appropriate;
xv. it is necessary to protect your or another person's vital interests, for example, where you have a life-threatening accident or illness in the workplace and we have to process your personal data in order to ensure you receive appropriate medical attention;
xvi. it is necessary for the establishment, exercise or defence of legal claims, such as where any person has brought a claim or serious complaint against us or you.

We also process personal data to comply with our legal obligations, notably those in connection with employment, company law, tax law and accounting, and child welfare. In this respect, depending on role and status, we are likely to use personal data for the following:

xvii. to meet our legal obligations (for example, relating to child welfare, social protection, diversity, equality, and gender pay gap monitoring, employment, and health and safety);
xviii. for tax and accounting purposes, including transferring personal data to HM Revenue and Customs to ensure that you have paid appropriate amounts of tax, and in respect of any Gift Aid claims, where relevant;
xix. for the prevention and detection of crime, and in order to assist with investigations (including criminal investigations) carried out by the police and other competent authorities.

f. Sharing your information with others

For the purposes referred to in this privacy notice and relying on the bases for processing as set out above, we may share your personal data with certain third parties. We may disclose limited personal data (including in limited cases special category or criminal data) to a variety of recipients including:

i. other employees, agents and contractors (eg third parties processing data on our behalf as part of administering payroll services, the provision of benefits including pensions, IT etc. – although this is not sharing your data in a legal sense, as these are considered data processors on our behalf);
ii. DBS and other relevant authorities and agencies such as the Department for Education, NCTL, the ICO, and the local authority;
iii. other settings in The Group
iv. external auditors or inspectors;
v. our advisers where it is necessary for us to obtain their advice or assistance, including insurers, lawyers, accountants, or other external consultants;
vi. third parties and their advisers in the unlikely event that those third parties are acquiring or considering acquiring all or part of The Group, or we are reconstituting or setting up some form of joint working or partnership arrangement in the unlikely event that those third parties are acquiring or considering acquiring all or part of The Group, or we are reconstituting.

vii. when The Group is legally required to do so (by a court order, government body, law enforcement agency or other authority of competent jurisdiction), for example HM Revenue and Customs or police.

viii. We may also share information about you with other employers in the form of a reference, where we consider it appropriate, or if we are required to do so in compliance with our legal obligations. References given or received in confidence may not be accessible under your GDPR rights.

g. Data retention

i. Personal data relating to unsuccessful job applicants is deleted within 6 months except where we have notified you we intend to keep it for longer (and you have not objected).

ii. Subject to any other notices that we may provide to you, we may retain your personal data for a period of seven years after your contract has expired or been terminated.

iii. However, some information may be retained for longer than this, for example incident reports and safeguarding files, in accordance with specific legal requirements.

h. Your rights

Please see our External Privacy Notice which has details of your rights as a 'data subject', which are the same as if you were any member for the public. You can find out more about your rights under applicable data protection legislation from the Information Commissioner's Office website available at www.ico.org.uk.

i. Contact and complaints

If you have any queries about this privacy notice or how we process your personal data, or if you wish to exercise any of your rights under applicable law, you may contact dataprotection@wishford.co.uk.

If you are not satisfied with how we are processing your personal data, or how we deal with your complaint, you can make a complaint to the Information Commissioner: www.ico.org.uk. The ICO does recommend you seek to resolve any issues with the data controller initially prior to any referral.

5. CCTV Procedures

- The purpose of this appendix is to regulate the management and operation of any Closed Circuit Television (CCTV) System at any Wishford setting. It also serves as a notice and a guide to data subjects (including pupils, parents, staff, volunteers, visitors to the Setting and members of the public) regarding their rights in relation to personal data recorded via any CCTV system (the **System**).

- Systems are administered and managed by the Wishford Education (Group) Ltd, who act as the Data Controller. This procedure will be reviewed alongside the overall Data Protection policy or sooner if legislation dictates. For further guidance, please review the Information Commissioner's CCTV Code of Practice.

- All fixed cameras are in plain sight of Setting premises and our Settings do not use CCTV for covert monitoring or routine monitoring of private property outside the grounds.

- The group's purposes for using the CCTV system are set out below and, having fully considered the privacy rights of individuals, the group believes these purposes are all in its legitimate interests. Data captured for the purposes below will not be used for any commercial purpose.

1. Objectives of our CCTV systems

- To protect pupils, staff, volunteers, visitors and members of the public, with regard to their personal safety.
- To protect buildings and equipment, and the personal property of pupils, staff, volunteers, visitors and members of the public.
- To support the police and community in preventing and detecting crime, and assist in the identification and apprehension of offenders.
- To monitor the security and integrity of the site.
- To monitor staff and contractors when carrying out work duties.

2. Positioning

- In settings where CCTV has been installed, locations have been be selected, both inside and out, that the setting reasonably believes require monitoring to address the stated objectives.
- Adequate signage has been placed in prominent positions to inform staff and pupils that they are entering a monitored area, identifying the Setting as the Data Controller and giving contact details for further information regarding the system.
- No images will be captured from areas in which individuals would have a heightened expectation of privacy, including changing and washroom facilities.
- No images of public spaces will be captured except to a limited extent at site entrances.

3. Maintenance

- Our CCTV Systems are operational 24 hours a day, every day of the year.
- The Group will appoint a System Manager who will check and confirm that the System is properly recording and that cameras are functioning correctly, on a regular basis.
- Every system will be checked and (to the extent necessary) serviced no less than annually.

4. Supervision of the System

- Staff authorised by the System Manager to conduct routine supervision of the System may include site staff, day or night security, supervisors at the sports centre and relevant staff on duty.
- Images will be viewed and/or monitored in a suitably secure and private area to minimise the likelihood of or opportunity for access to unauthorised persons.

5. Storage of Data

- The day-to-day management of images will be the responsibility of the System Manager, or such suitable person as the System Manager shall appoint in his or her absence.
- Images will be stored for 28 days and automatically over-written unless the setting considers it reasonably necessary for the pursuit of the objectives outlined above, or if lawfully required by an appropriate third party such as the police or local authority.
- Where such data is retained, it will be retained in accordance with the Act and our Data Protection Policy. Information including the date, time and length of the recording, as well as the locations covered and groups or individuals recorded, will be recorded in the system log book.

6. Access to Images

- Access to stored CCTV images will only be given to authorised persons, under the supervision of the System Manager, in pursuance of the above objectives (or if there is some other overriding and lawful reason to grant such access).
- Individuals also have the right to access personal data The Group holds on them, including information held on the System, if it has been kept. The Group will require specific details including at least to time, date and camera location before it can properly respond to any such requests (see appendix 1 below). This right is subject to certain exemptions from access, including in some circumstances where others are identifiable.
- The System Manager must satisfy themselves of the identity of any person wishing to view stored images or access the system and the legitimacy of the request. The following are examples when the System Manager may authorise access to CCTV images:
    - Where required to do so by the Head, the Police or some relevant statutory authority;
    - To make a report regarding suspected criminal behaviour;
    - To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
    - To assist the Setting in establishing facts in cases of unacceptable pupil behaviour, in which case, the parents/guardian will be informed as part of the Setting's management of a particular incident;
    - To data subjects (or their legal representatives) pursuant to an access request under the Act and on the basis set out above;
    - To the Group's insurance company where required in order to pursue a claim for damage done to insured property; or
    - In any other circumstances required under law or regulation.
- Where images are disclosed, a record will be made in the system log book including the person viewing the images, the time of access, the reason for viewing the images, the details of images viewed and a crime incident number (if applicable).

7 Other CCTV systems

Our settings do not own or manage third party CCTV systems.

8 Complaints and queries

- Any complaints or queries in relation to the Setting's CCTV system, or its use of CCTV, or requests for copies, should be referred to the Group's Data Protection Officer (data.protection@wishford.co.uk).
- For any other queries concerning the use of your personal data by the Setting, please see the External Privacy Notice.

APPENDIX 1: CCTV FOOTAGE ACCESS REQUEST

The following information is required before a setting can provide copies of or access to CCTV footage from which a person believes they may be identified.

Please note that CCTV footage may contain the information of others that needs to be protected, and that the setting typically deletes CCTV recordings after 28 days.

Name and address: (proof of ID may be required)	
Description of footage (including a description of yourself, clothing, activity etc.)	
Location of camera	
Date of footage sought	
Approximate time (give a range if necessary)	

Signature*……

Print Name……. Date ……..

*** NB if requesting CCTV footage of a child [under 12 / 13 / of preparatory school age], a person with parental responsibility should sign this form. For children [over that age / at secondary school], the child's authority or consent must be obtained except in circumstances where that would clearly be inappropriate and the lawful reasons to provide to the parent(s) outweigh the privacy considerations of the child.**

APPENDIX 2: TEMPLATE DATA PROCESSING AGREEMENT PRECEDENT

[SETTING] IS CONTROLLER AND [SUPPLIER] IS PROCESSOR

Guidance note: this long-form data processing agreement may be used either as a stand-alone contract, with sufficient descriptions and instructions as the nature of the processing (for example in the Schedule); or in conjunction with (or as a Schedule or Addendum to) an existing or parallel Service Agreement containing its own commercial terms.

Settings should be careful to consider and indicate which takes priority in event of any contradiction or overlap between the two (see clause 1.14): and we strongly recommend that, in respect of data protection or privacy issues, it should be this Agreement.

ISBA has worked in conjunction with Farrer & Co on this document. This document is not a substitute for legal advice.

BACKGROUND

[INCLUDE AS BACKGROUND THE FACT THAT THE SETTING AND THE SUPPLIER HAVE ENTERED INTO A SEPARATE SUPPLY / SERVICE AGREEMENT, ON WHAT DATE, AND TO PROVIDE WHAT SERVICES]

(A) This Agreement is to ensure the protection and security of Personal Data that is the subject of the [Service Agreement], including all Personal Data passed from the Setting (Data Controller) to the Supplier (Data Processor) for processing, or accessed by the Supplier on the Setting's authority for processing, or otherwise received by the Supplier for processing on the Setting's behalf;

(B) The Data Protection Laws place certain obligations upon a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to ensure that the processing of the Personal Data carried out on its behalf is secure;

(C) This Agreement exists further to ensure that there are sufficient security guarantees in place and that the processing complies with obligations equivalent to those required by the Data Protection Laws;

(D) This Agreement further defines certain service levels to be applied to all uses of Personal Data and all Personal Data related services provided by the Supplier.

(E) Definitions in this Background have the meanings given in the Agreement and/or the Data Protection Laws.

Data Protection

Definitions

In this Agreement:

Data means all Personal Data collected, generated or otherwise processed by Supplier as a result of, or in connection with, the provision of the Services.

Data Protection Laws means:

the Data Protection Act 2018;

the General Data Protection Regulation (EU 2016/679) (GDPR) and any legislation which amends, re-enacts or replaces it in England and Wales;

the Electronic Communications (EC Directive) Regulations 2003, together with any legislation which replaces it; and

at all times, any other data protection laws and regulations applicable in England and Wales.

[Data Protection Officer has the meaning given to it under Article 37 of GDPR.][1]

Data Subject means an individual who is the subject of personal data.

[EEA means the European Economic Area.]

[Losses means costs, claims, demands, actions, awards, judgments, settlements, expenses, liabilities, damages and losses (including all interest, fines, penalties, management time and legal and other professional costs and expenses).][2]

Personal Data has the meaning given to it under the Data Protection Laws.

Records means the records referred to in Clause 1.7.1.

Services means [definition from Services Agreement or reflected here]

Services Agreement means [may be defined in Background above]

Sub-Processor has the meaning set out in Clause 1.4.1.

Supervisory Authority means any data protection authority with jurisdiction over the processing of the Data.

Data Processing

[Supplier] shall comply with the requirements of the Data Protection Laws in respect of the activities which are the subject of the Agreement and shall not knowingly do anything or permit anything to be done which might lead to a breach by [Setting] of the Data Protection Laws.

[Supplier] may only process Data to the extent it relates to:

the types of Data;

the categories of Data Subject;

the nature and purpose,

set out in Schedule [●] and only for the duration specified therein.[3]

Without prejudice to Clause 1.2.1 [Supplier] shall:

process the Data only in accordance with the written instructions of [Setting], unless [Supplier] is required to process the Data for other reasons under the laws of the European Union (or a member state of the European Union) to which [Supplier] is subject. If [Supplier] is required to process the Data for these other reasons, [Supplier] shall inform [Setting] before carrying out the processing, unless prohibited by relevant law.[4]

immediately inform [Setting] if it believes that [Setting]'s instructions infringe the Data Protection Laws;

[1] May or may not be relevant to either Setting or Supplier (Data Processor). Please see the ISBA note on this topic and seek advice if unsure.
[2] May be included in definitions if there are other indemnities in the applicable Services Agreement.
[3] Either the Schedule or the applicable service contract (or both) will need to deal with these issues in some detail and possibly allow for flexibility as needs change.
[4] Article 28(3)(a) GDPR.

have in place, and maintain throughout the term at all times in accordance with the then current [best industry practice/good industry practice], all appropriate technical and organisational security measures against:

unauthorised or unlawful processing, use, access to or theft of the Data; and

loss or destruction of or damage to the Data,

to ensure that [Supplier]'s processing of the Data is in accordance with the requirements of the Data Protection Laws and protects the rights of the Data Subjects. On request [Supplier] shall provide [Setting] with a current written description of the security measures being taken;[5]

ensure that all persons authorised by [Supplier] to process Data are bound by obligations equivalent to those set out in this Clause 1;[6]

ensure that access to the Data is limited to:

those [Supplier] personnel who need access to the Data to meet [Supplier]'s obligations under the Agreement; and

in the case of any access by any [Supplier] personnel, such Data as is strictly necessary for performance of that [Supplier] personnel's duties;[7]

[*ONLY APPLICABLE WHERE [SUPPLIER] IS NOT ESTABLISHED IN THE EU*] [nominate a representative based in the European Union, [to the extent required for [Supplier] to comply with the Data Protection Laws;][8] and

if required under the Data Protection Laws, appoint a Data Protection Officer.[9]

[Supplier] shall provide such assistance as [Setting] requires in order for [Setting] to:

respond to requests relating to [Supplier]'s data processing from Data Subjects;[10]

ensure compliance with [Setting]'s obligations under the Data Protection Laws, including in relation to:

the security of processing; and

with the preparation of any necessary data protection impact assessments and the undertaking of any necessary data protection consultations.[11]

Transfers Outside of the EEA

[Supplier] shall not allow any Data to be processed or transferred to any country outside of the EEA [other than to the UK] unless:

it notifies [Setting] in writing that it intends to transfer any Data outside of the EEA [other than to the UK];

[Setting] provides its written consent to such transfer (which consent it may give or withhold in its absolute discretion); and

it provides in advance of a transfer authorised under Clause 1.3.1(b) evidence to the [Setting]'s satisfaction of appropriate safeguards, as required by Data Protection Laws.

---

[5] Article 28(1) GDPR.
[6] Article 28(3)(b) GDPR.
[7] Not strictly required by GDPR but recommended to supplement (d).
[8] Article 27 GDPR
[9] Article 27 GDPR
[10] Article 28(3)(e) GDPR
[11] Article 28(3)(f) GDPR

[Failure to comply with this Clause 1.3 shall be deemed a material breach of [this Agreement] OR [the Services Agreement] incapable of remedy.[12]

Sub-Processors[13]

[Supplier] shall not engage any third party, [except OR including a member of [Supplier]'s group], to carry out processing in connection with the Services (Sub-Processor) without [Setting]'s prior written consent.[14] [For the purposes of this Clause 1.4.1, [name(s) of Sub-Processor OR those Sub-Processors listed in Annex X] shall be deemed approved by the Setting. For the avoidance of doubt, this Clause 1.4.1 shall also apply to any replacement Sub-Processor.

Prior to allowing a Sub-Processor authorised under or in accordance with Clause 1.4.1, including any member of [Supplier's] group, to process any Data, [Supplier] shall enter into a written agreement with the Sub-Processor under which Sub-Processor is obliged to comply with the terms of this Clause 1. [Supplier] remains fully liable to [Setting] for any acts or omissions of any Sub-Processors.[15]

Information Provision and Data Protection Audits[16]

On request and at no additional charge, [Supplier] shall provide to [Setting] all information required by [Setting] to assess [Supplier]'s compliance with Clause 1 and the Data Protection Laws and, to the extent possible, all information necessary for [Setting] to demonstrate [Setting]'s compliance with the Data Protection Laws;[17] and

In order that [Setting] [and/or its authorised representative] and any Supervisory Authority may audit [Supplier]'s compliance with the Data Protection Laws and the terms of this Clause 1, on request and at no additional charge [Supplier] shall provide [Setting] with:

reasonable access to all relevant information, premises, Data, employees, agents, [Supplier] Sub-Processors and assets at all locations from which obligations of [Supplier] under this Clause 1 are being or have been or should have been carried out; and

all reasonable assistance in carrying out the audit,

during the Term and for [36] months after the Termination Date, subject to [Setting] giving [Supplier] [five] [Business Days']/[seven days'] notice (except where such audit is required by a Supervisory Authority to which [Setting] is subject).[18]

Dealings with Supervisory Authorities

[Supplier] shall promptly provide all assistance and information which is requested by any Supervisory Authority.[19]

[Supplier] shall immediately notify [Setting] of any request that it receives from any Supervisory Authority for assistance or information, unless prohibited by relevant law.

Records [20]

---

[12] This can be cross-referenced to the Setting's rights under the Services Agreement
[13] Guidance note: any subcontracting clause should be subject to these sub-processor provisions.
[14] Article 28(2) GDPR. It is also possible for the Setting to give a general **consent** to sub-processing, but this risks complicating matters as the Setting must still be notified and also retain a right to object.
[15] Article 28(3)(d) and Article 28(4) GDPR
[16] Guidance Note: any more general audit wording in the Services Agreement should not contradict this clause. Specific governing law requirements for data protection clauses may mean that, following Brexit, an English law governed audit clause is insufficient for EU law.
[17] Article 28(3)(h) GDPR
[18] Article 28(3)(h) GDPR
[19] Article 31 GDPR
[20] Guidance note: Guidance note: GDPR has specific requirements for record keeping by data processors. Any more general records wording in e.g. the main Service Agreement should not contradict it and, as far as data processing records are concerned, these should take precedence.

[Supplier] shall maintain records of all processing activities carried out on behalf of [Setting], [21] including:

the information described in Clause 1.5;

where applicable, the name and contact details of the Data Protection Officer [or representative based in the European Union][22] of [Supplier] and of any sub-processors;

the different types of processing being carried out (if applicable);

any transfers of Data outside of the EEA [or UK], including the identification of the relevant country or international organisation and any documentation required to demonstrate suitable safeguards;

a description of the technical and organisational security measures referred to in Clause 1.2.3,

together, the Records (Records).

The Records shall be in written electronic form.

[Supplier] shall provide the Records to [Setting] promptly on request.

Data Subjects

On request, [Supplier] shall take all necessary action and provide [Setting] with all reasonable assistance necessary for [Setting] to comply with [Setting]'s obligations under the Data Protection Laws in relation to:

the provision of information to Data Subjects;[23]

the rectification of inaccurate Data in relation to a Data Subject;[24]

the erasure of a Data Subject's Data;[25] and

the retrieval and transfer of the Data of a Data Subject.[26]

Data Breaches

[Supplier] shall notify [Setting] immediately after becoming aware of any unauthorised or unlawful processing, use of, or access to the Data, or any theft of, loss of, damage to or destruction of the Data (Security Incident) or any breach of this Clause 1.[27] [Failure to notify [Setting] shall be deemed a material breach of the Service Agreement under Clause [●] incapable of remedy.[28]

[In the event of a Security Incident, [Supplier] shall provide [Setting] with full co-operation and assistance in dealing with the Security Incident, in particular in relation to:

resolving any data privacy or security issues involving any Data; and

making any appropriate notifications to individuals affected by the Security Incident or to a Supervisory Authority.

[Supplier] shall investigate the Security Incident in the most expedient time possible and shall then provide [Setting] as soon as possible thereafter with a detailed description of the Security Incident, the

[21] Reflects requirements of Article 30. These obligations apply to any data processor employing 250 persons or more; or if the processing it carries out is likely to result in a risk to the right and freedoms of Data Subjects; or if the processing is not occasional; or if the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
[22] Include where [Supplier] is not established in the EU.
[23] Article 12 GDPR.
[24] Article 16 GDPR.
[25] Article 17 GDPR.
[26] Article 20 GDPR.
[27] Article 33(2) GDPR
[28] Add appropriate cross-reference to any provision in the Service Agreement.

type of data that was the subject of the Security Incident, and any other information that [Setting] may request concerning the Security Incident.

[Supplier] shall take all steps necessary to prevent a repeat of the Security Incident and shall consult with and agree those steps with the [Setting] unless immediate steps need to be taken and it is impractical to consult with [Setting] in that respect.][29]

Return or Destruction of Data

[Supplier] shall, at [Setting]'s discretion, destroy or return all Data to [Setting] on termination of this Agreement, and shall destroy or delete all copies it holds of the Data, unless relevant local law to which [Supplier] is subject requires that Data to be retained.[30]

Governing Law

If it is or becomes a requirement that, under the Data Protection Laws or other Applicable Laws, Clause 1 must be governed by the laws of a member state of the European Union, and the governing law specified in Clause [●] does not or ceases to satisfy this requirement, Clause 1 shall be governed by and construed in accordance with the laws of [●].[31]

[Warranties[32]

The Supplier (Data Processor) warrants that:

it will process the Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments, including the Data Protection Laws; and

it will take appropriate technical and organisational measures against the unauthorised or unlawful processing of Data and against the accidental loss or destruction of, or damage to Data to ensure the Setting's compliance with the Data Protection Laws.

The Supplier shall notify the Setting immediately if it becomes aware of:

any unauthorised or unlawful processing, loss of, damage to or destruction of the Data;

any advance in technology and best practice which mean that the Setting should revise the security and technical measures in place in order to protect the Data as well as the processing of the Data.

The Data Controller (Setting) warrants that:

it will provide the Supplier with all Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments, including Data Protection Laws; and

the Data which it supplies or discloses to the Supplier, has been obtained fairly and lawfully; and

it will obtain all necessary consents from persons whose Data is being processed and registrations with authorities to permit the Setting to transfer Personal Data to third parties pursuant to its obligations under this Agreement.]

Indemnity

[29] The inclusion of these provisions is not expressly required by GDPR, but recommended where the personal data being processed is high volume or of any sensitivity.
[30] Article 28(3)(g) GDPR.
[31] Reflects requirements of Article 38(3) GDPR and uncertainties associated with UK leaving EU. Relevant jurisdiction to be considered on a case by case basis and GDPR requirement for law to be governed under an EU country. Post-Brexit provisions may or may not be made to allow the UK to qualify. In many cases Irish law may be the most appropriate alternative.
[32] This section is, in essence, a short-form of the general obligations of the Agreement and may either reinforce the main obligations or be used as the basis for a more light-touch, shorter data processing agreement. However it in no way fulfils all the requirements of GDPR and advice should be sought before removing provisions, shortening or otherwise amending this Agreement.

[Supplier] shall on demand indemnify [Setting] from and against all Losses incurred by [Setting], or its employees, officers, agents and contractors] as a result of any breach by [Supplier] (or any entity or individual appointed by [Supplier] to carry out its obligations) of Clause 1.

Priority

[Supplier] shall comply with this Agreement in addition to its obligations under any other contract with the [Setting] (whether currently in force or entered into in the future). Where there is any inconsistency between the two, in relation to [data protection law] [confidential information] this Agreement shall prevail, unless the [Setting] notifies the [Supplier] otherwise in writing.

Data Processing

Type of Data to be Processed

[●].

Categories of Data Subject whose Data will be Processed

[●].

Nature and Purpose of Processing

[●].

Duration of Processing

[●].