PRIVACY NOTICE

DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: 1. Name (including initials) 2. Identification number 3. Location data 4. Online identifier, such as a username 5. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: 1. Racial or ethnic origin 2. Political opinions 3. Religious or philosophical beliefs 4. Trade union membership 5. Genetics 6. Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes 7. Health – physical or mental 8. Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Who processes your information?
hubulu.com Ltd is the data controller of the personal information you provide to us. This means the company determines the purposes for which, and the manner in which, any personal data relating to clients is processed.

Ms Sarah Broadfoot, hubulu.com Ltd, 7 Filluel Road WAREHAM BH20 7AW acts as a representative for the company with regard to its data controller responsibilities; they can be contacted on 07969 925993 or info@hubulu.com

In some cases, your data will be outsourced to a third-party processor; however, this will only be done with your consent, unless the law requires the company to share your data. Where the company outsources data to a third-party processor, the same data protection standards that hubulu.com Ltd upholds are imposed on the processor.

The role of the Data Protection Officer (DPO) is to oversee and monitor the company's data protection procedures, and to ensure they are compliant with the GDPR. You can also find out about the General Data Protection Regulations and Data Protection Act 2018 and your rights on the Information Commissioners Website www.ico.org.uk

Why do we collect and use your information?
hubulu.com Ltd holds the legal right to collect and use personal data relating to our clients (for whom we also act on behalf of as a third party, trading as Your Clerk) and our staff. The personal data of clients is collected and used for the following reasons:

1. To fulfil the role of which we have be appointed to by the client to undertake
2. To contact the client about their booking(s) and the service(s) they receive from us
3. To inform the client about when their next service appointment is due; special offers and discounts; company news and updates
4. To assess the quality of our service

For Your Clerk, we may also receive information regarding them from their previous company, local authority and the Department of Education (DfE). We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK law, including those in relation to the following:

1. Article 6 and Article 9 of the GDPR
2. Education Act 1996
3. Regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013

In accordance with the above, the personal data of clients, members Governing Bodies, Local Advisory Boards, Local Governing Boards, Trust Board and Boards of Directors is collected and used for the following reasons:

5. To fulfil the role of which we have be appointed to by our client to undertake
6. To report back to the DfE and provide statutory information required to be displayed by our clients on their websites
7. To monitor and report on attendance
8. To monitor and report on pecuniary and business interests
9. To assist our client in meeting statutory requirements for school governance
10. To comply with the law regarding data sharing, including sharing data with the local authority and Department of Education
11. To assess the quality of our service

What data is collected?
The categories of information that the company collects, holds and shares includes **personal information**, such as:

1. name(s)
2. contact telephone number(s)
3. emails address(es)
4. postal address(es)
5. date of birth

In order to fulfil the function of Your Clerk, we also collect data on:

1. meeting attendance
2. committee membership
3. length of service
4. pecuniary and business interests

Whilst the majority of the personal data you provide to the company is mandatory for clients of Your Clerk, some is provided on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

How long is your data stored for?

Personal data relating to is stored in line with the company's Data Protection Policy. We keep information about you on computer systems and sometimes on paper. We hold records securely for a maximum period of seven years, after which they are safely destroyed. In accordance with the General Data Protection Regulation (GDPR), the company does not store personal data indefinitely; data is only stored for as long as is necessary to complete the task for which it was originally collected.

The lawful basis on which we use this information

Trading as Your Clerk, we have a legal obligation to collect and use School Governor/Director information under the Education Act 1996. The legal reason for us to collect and use this personal information is to enable our clients to perform their statutory duties and it is required by law and for reasons of public interest.

Whilst the majority of information you provide to us is mandatory for clients of Your Clerk, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this. It is possible to refuse to provide data on nationality and country of birth, please contact us if you wish to discuss this.

Will my information be shared?

hubulu.com Ltd will not share your personal information with any third parties without your consent, unless the law and our policies allows us to do so. Trading as Your Clerk, the company routinely shares Governor/Director information with:

1. our client (i.e. the school or Academy Trust for whom who are Governor/Director)
2. the Local Authority and/or Academy Trust Board
3. the Department of Education

Clients of Your Clerk: we share your data with our client and the local authority on a statutory basis. There are several acts and regulations that require the sharing of data between schools (whom we represent) and the local authority including;

- Education Act 1996
- Education Act 2002
- Education and Inspections Act 2006
- Education (Pupil Registration) (England) Regulations 2006
- Education (Information About Individual Pupils) (England) Regulations 2013

- Education (Pupil Registration) (Amendment) (England) Regulations 2016
- Education Act 2002, as amended by the Education Act 2011;
- Company Discipline (Pupil Exclusions and Reviews) (England) Regulations 2012;
- Education (Provision of Full-Time Education for Excluded Pupils) (England) Regulations 2007, as amended by the Education (Provision of Full-Time Education for Excluded Pupils) (England) (Amendment) Regulations 2014.

The local authority also provides information to the Health Service on behalf of the school (whom we represent). Where-ever possible this data is anonymised before sharing.

Data collection requirements
To find out more about the data collection requirements placed on us by the Department for Education please visit www.gov.uk/education/data-collection-and-censuses-for-schools

DfE's National Database
Trading as Your Clerk, the company is required to share Governor/Director data with the Department for Education (DfE) on a statutory basis. The database is owned and managed by the DfE and contains information about Governors/Directors of all schools and Academy Trusts in England. It is held in electronic format for statistical and safeguarding purposes. This information is securely collected from a range of sources including schools (and their representatives), local authorities and awarding bodies.

hubulu.com Ltd is required by law to provide information about our (Your Clerk) clients to the DfE as part of statutory data collections; some of this information is then stored in the DfE's database. The DfE may share information about our clients with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- Who is requesting the data
- The purpose for which it is required
- The level and sensitivity of data requested
- The arrangements in place to store and handle the data

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data. For more information about the department's data sharing process, please visit: www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

What are your rights?
Our clients have the following rights in relation to the processing of their personal data. You have the right to:

1. Be informed about how hubulu.com Ltd uses your personal data
2. Request access to the personal data that hubulu.com Ltd holds
3. Request that your personal data is amended if it is inaccurate or incomplete
4. Request that your personal data is erased where there is no compelling reason for its continued processing

5. Request that the processing of your data is restricted
6. Object to your personal data being processed

To make a request for your personal information, please contact our Data Protection Officer. Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.

If you have a concern about the way hubulu.com Ltd and/or the DfE is collecting or using your personal data, you can raise a concern with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm or via the website www.ico.org.uk

APPENDIX 1

PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Officer (DPO). The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

1. Lost
2. Stolen
3. Destroyed
4. Altered
5. Disclosed or made available where it should not have been
6. Made available to unauthorised people

The DPO will alert the Managing Director and any client(s) affected by the breach. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure). The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.

The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

1. Loss of control over their data
2. Discrimination
3. Identify theft or fraud
4. Financial loss
5. Unauthorised reversal of pseudonymisation (for example, key-coding)
6. Damage to reputation
7. Loss of confidentiality
8. Any other significant economic or social disadvantage to the individual(s) concerned

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the company's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72-hours. As required, the DPO will set out:

1. A description of the nature of the personal data breach including, where possible:
2. The categories and approximate number of individuals concerned
3. The categories and approximate number of personal data records concerned
4. The name and contact details of the DPO
5. A description of the likely consequences of the personal data breach
6. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the above details are not yet known, the DPO will report as much as they can within 72-hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

1. The name and contact details of the DPO
2. A description of the likely consequences of the personal data breach
3. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

The DPO will notify any relevant third parties who can help mitigate the loss to individuals, for example, the police, insurers, banks or credit card companies. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

1. Facts and cause
2. Effects
3. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the company's computer system. The DPO and client(s) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

1. If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
2. Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
3. If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it
4. In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
5. The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
6. The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted