DATA PROTECTION POLICY

1. 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.

2. ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our company, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

3. COLLECTING PERSONAL DATA

3.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that the company can **fulfil a contract** with the individual, or the individual has asked the company to take specific steps before entering into a contract
2. The data needs to be processed so that the company can **comply with a legal obligation**
3. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
4. The data needs to be processed so that the company, as a public authority, can perform a task **in the public interest,** and carry out its official functions
5. The data needs to be processed for the **legitimate interests** of the company or a third party (provided the individual's rights and freedoms are not overridden)
6. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

3.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

4. SHARING PERSONAL DATA

hubulu.com Ltd does not normally share personal data with anyone else, but we may do so where:

1. There is an issue with a that puts the safety of our staff at risk
2. We need to liaise with other agencies – we will seek consent as necessary before doing this
3. Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies.

When doing this, we will:

1. Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
2. Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
3. Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

1. The prevention or detection of crime and/or fraud
2. The apprehension or prosecution of offenders
3. The assessment or collection of tax owed to HMRC
4. In connection with legal proceedings
5. Where the disclosure is required to satisfy our safeguarding obligations

6. Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our clients. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

5. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

5.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the company holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter or email to the appointed Data Protection Officer (DPO). They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request they must immediately forward it to the DPO.

5.2 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via telephone to confirm the request was made
- Will respond without delay and within 30-days of receipt of the request
- Will provide the information free of charge*
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the client or another individual
- Would reveal that a client is at risk of abuse, where the disclosure of that information would not be in the client's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning a client
- If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs
- A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the Information Commissioner's Office (ICO).

* a fee may apply to cover the reasonable costs of administrative work associated with processing the request

5.3 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

6. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

1. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
2. Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
3. Where personal information needs to be taken off site, staff must sign it in and out from the company office
4. Passwords that are at least eight characters long containing letters, numbers and special characters are used to access company computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
5. Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
6. Staff who store personal information on their personal devices are expected to follow the same security procedures as for company-owned equipment
7. Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

7. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred or incinerate paper-based records, and overwrite or delete electronic

files. We may also use a third party to safely dispose of records on the company's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

8. PERSONAL DATA BREACHES

The company will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service.

When appropriate, we will report the data breach to the ICO within 72- hours.

9. USE OF COOKIES

We're committed to protecting your personal information and ensuring your experience with us is as safe and enjoyable as possible. In this section, you'll find information on how and why we collect, store and use personal information to improve our service. You'll also find out how to manage the information that's collected.

Most websites use cookies to improve your browsing experience. Cookies are small amounts of information in the form of text files sent by our website (or the website of a company we have a relationship with) to your computer, mobile phone or other device when you visit our website. They allow us to do various things, including tailor the content you see, and ensure the security of your Online Service experience.

We use a combination of different cookies to improve your Online Service experience. A cookie allows us to remember your previous choices on our site, so you don't have to repeat them on each visit. Here is a list of the cookies in use on our websites:

COOKIE NAME	LIFE SPAN	PURPOSE
svSession	Permanent	Creates activities and BI
hs	Session	Security
incap_ses_${Proxy-ID}_${Site-ID}	Session	Security
incap_visid_${Proxy-ID}_${Site-ID}	Session	Security
nlbi_{ID}	Persistent cookie	Security
XSRF-TOKEN	Persistent cookie	Security
smSession	Two weeks	Identify logged in site members

9.1 Session Cookies

Session cookies last only for the duration of your visit and are deleted when you close your browser. These facilitate various tasks such as allowing a website to identify that a user of a particular device is navigating from page to page, supporting website security or basic functionality. Many of the cookies we use are session cookies. For example, they help us to ensure the security of your Online Service session, and can also keep you signed in to Online Service while you move between pages or service your account.

9.2 First and Third-Party Cookies

Whether a cookie is a first or third party cookie depends on which website the cookie comes from. First party cookies are those set by or on behalf of the website visited. All other cookies are third party cookies. We use both first party and third party cookies.

9.3 restricting or blocking cookies

You can choose to restrict or block the cookies set by us, or any website. You'll need to do this through your

browser settings. Please note, if you block or restrict cookies on your machine, the hubulu.com Ltd online services may not function correctly.

Your browser settings are usually found in the 'options' or 'preferences' menu. The Help function in your browser will show you how to change the settings. We use cookies to provide and maintain a secure environment for your Online service, to protect you from fraud. However, you can make hubulu.com Ltd a trusted website in your browser settings so that each time you visit, your cookies are enabled for hubulu.com Ltd and will allow Online Service to work.

If your concern is with third party cookies generated by advertisers, you can turn these off by going to the third party's website and getting it to generate a one-time 'no thanks' cookie, to stop any further cookies being served to your machine. Remember, for cookie blocking or restrictions, you'll need to adjust the browser settings on every device you use for internet access.

You can also visit www.allaboutcookies.org for comprehensive information on how to block or restrict cookies on a wide variety of browsers. You'll also find details on how to delete cookies from your computer, as well as more general information about cookies. For information on how to do this on the browser of your mobile phone you'll need to refer to your handset manual.

9. CONTACT

Ms Sarah Broadfoot, hubulu.com Ltd, 7 Filleul 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