JellyJames Data Protection Policy

1. **Introduction**

This Policy sets out the obligations of JellyJames Publishing Ltd, a company registered in the United Kingdom under number 07136009, regarding data protection and the rights of clients, end users of our online products, and JellyJames Publishing Ltd employees and contracted personnel ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The Company is a data controller in respect of information such as Company personnel data and marketing data, and a data processor in respect of information such as data transmitted and displayed on its mobile app products supplied to clients (see Part 20).

This Policy sets the Company's obligations as a data controller and data processor regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. **The Data Protection Principles**

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

a. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
b. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
d. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.
f. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. **The Rights of Data Subjects**

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

a. The right to be informed (Part 12).
b. The right of access (Part 13);
c. The right to rectification (Part 14);
d. The right to erasure (also known as the 'right to be forgotten') (Part 15);
e. The right to restrict processing (Part 16);
f. The right to data portability (Part 17);
g. The right to object (Part 18); and
h. Rights with respect to automated decision-making (Part 19).

4. **Lawful, Fair, and Transparent Data Processing**

a. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
    1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
    2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
    3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
    4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
    5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
    6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
b. If the personal data in question is "special category data" (also known as "sensitive personal data") (for example, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
    1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
    2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
    3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
    4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
    5. The processing relates to personal data which is clearly made public by the data subject;
    6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

7. The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
9. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5. **Specified, Explicit, and Legitimate Purposes**

a. The Company collects and processes the personal data set out in Part 20 of this Policy. This includes: Personal data collected directly from data subjects; and Personal data obtained from third parties.
b. The Company only collects, processes, and holds personal data for the specific purposes set out in Part 20 of this Policy (or for other purposes expressly permitted by the GDPR).
c. Data subjects are kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. **Adequate, Relevant, and Limited Data Processing**

The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 5, above, and as set out in Part 20, below.

7. **Accuracy of Data and Keeping Data Up-to-Date**

a. In cases when the Company is the data controller:
   1. The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 14, below.
   2. The accuracy of personal data shall be checked when it is collected and periodically thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.
b. In cases when the Company is the data processor the Company shall not check that all personal data processed, and held by it is accurate and up-to-date. but will assist the data controller to rectify personal data at the request of a data subject, as set out in Part 14, below, if required

8. **Data Retention**

a. The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.

b. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it within 12 months thereafter, subject to any legal obligation on JellyJames Publishing to retain the personal data.

9. **Secure Processing**

The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 21 to 28 of this Policy.

10. **Accountability and Record-Keeping**

a. The Company's Data Protection Officer (DPO) is Karim Esmail – Head of Technical Servives. Tel: 0203 113 2066
b. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.
c. In appointing a Data Protection Officer we have considered the following sources amongst others:
    1. Articles 37, 38 and 39 of the GDPR Regulation of the European Parliament, 27 April 2016
    2. ICO website, in particular its Data Protection Officers section
    3. The Article 29 Working Party guidelines on Data Protection Officers, 5 April 2017

The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a. The name and details of the Company, its Data Protection Officer, its Alternate Data Protection Officer and any applicable third-party data processors;
b. The purposes for which the Company collects, holds, and processes personal data;
c. Details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
d. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
e. Details of how long personal data will be retained by the Company; and
f. Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

11. **Data Protection Impact Assessments**

a. The Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which might result in a high risk to the rights and freedoms of data subjects under the GDPR.
b. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
    1. The type(s) of personal data that will be collected, held, and processed;
    2. The purpose(s) for which personal data is to be used;
    3. The Company's objectives;
    4. How personal data is to be used;
    5. The parties (internal and/or external) who are to be consulted;
    6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
    7. Risks posed to data subjects;
    8. Risks posed both within and to the Company; and
    9. Proposed measures to minimise and handle identified risks.

12. **Keeping Data Subjects Informed**

a. The Company shall provide the information set out in Part 12.2 to every data subject:
    1. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
    2. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
        I. if the personal data is used to communicate with the data subject, when the first communication is made; or
        II. if the personal data is to be transferred to another party, before that transfer is made; or
        III. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

b. The following information shall be provided:
    1. Details of the Company including, but not limited to, the identity of its Data Protection Officer;
    2. The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 20 of this Policy) and the legal basis justifying that collection and processing;
    3. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
    4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
    5. Where the personal data is to be transferred to one or more third parties, details of those parties;
    6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
    7. Details of data retention;
    8. Details of the data subject's rights under the GDPR;
    9. Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
    10. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
    11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
    12. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

13. **Data Subject Access**

a. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
b. Data subjects wishing to make a SAR may do so in writing, addressed to the Company's Data Protection Officer at JellyJames Publishing Ltd, Building 19, Cumberland Road, Stanmore HA7 1EL.
c. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
d. All SARs received shall be handled by the Company's Data Protection Officer.
e. The Company charges a fee for the handling of a SAR (see https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf). The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

14. **Rectification of Personal Data**

    a. Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
    b. The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    c. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

15. **Erasure of Personal Data**

    a. Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:
        1. It is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
        2. The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
        3. The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
        4. The personal data has been processed unlawfully;
        5. The personal data needs to be erased in order for the Company to comply with a particular legal obligation;
        6. The personal data is being held and processed for the purpose of providing information society services (online services) to a child.
    b. Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
    c. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. **Restriction of Personal Data Processing**

    a. Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
    b. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. **Data Portability**

    a. The Company processes personal data using automated means, for example automatically uploading personal data daily to the app's database.
    b. Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
    c. To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following Excel spreadsheet print out format.

d. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
e. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

18. **Objections to Personal Data Processing**

a. Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.
b. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
c. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.
d. Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the GDPR, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. **Automated Decision-Making**

a. The Company uses personal data in automated decision-making processes, for example in its email marketing activities.
b. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.
c. The right described in Part 19.2 does not apply in the following circumstances:
    1. The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;
    2. The decision is authorised by law; or
    3. The data subject has given their explicit consent.

20. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company:

	Type of data	Examples of data	Purpose
Data for which JellyJames Publishing Ltd is the data controller.			
20.1	Internal HR data	Employees' DOB; Passport number & expiry details; NI number; Tax Code and URN	HMRC / employment law requirements
20.2	Marketing lists	Headteachers', SENCos' Purchasing Managers, Parents and other client personal and work emails; work telephone numbers; work addresses	Marketing
20.3	Client data	Name, gender, position, email, telephone number	Necessary for operation of business

Data for which JellyJames Publishing Ltd is the data processor.			
20.4	Content Management System Users	Name, position, login name, password, email, telephone number, registration date, language, timezone	Authorising access for mobile and online apps administrators
20.5	Registration data (app end users)	Surname name, first name, year, class, group, connected persons' phone numbers and email addresses	Authorising access for end users
20.6	CMS Data	All content on online application (e.g. name, age, contact information etc.) all of which may include personal information if the data controller chooses to do so.	Information and messages on online apps
20.7	Performance and Assessment Results	Details contained in e.g. results of assessments taken and modules undertaken to carry or intervention work. All data in the application is managed by the account administrators.	Streamlining admin tasks

21. **Personal Data Shared With Sub-Processors**

The following Sub-Processors are used by the Company to collect, hold, and process data of which it is data controller and/or data processor. The Company will not use the services of any sub-processor which cannot demonstrate compliance with GDPR and other applicable data legislation.

	Sub-Processor	**Examples of data**	**Purpose**
21.1	Microsoft Office/Google Suite	Name, email, Google+ profile, Aliases, Storage, Apps enabled, Groups, Licences, Security Settings, Admin Roles, Devices assigned	Internal and external communication and workflow
21.2	Sage Act	Client contact details	CRM system
21.3	Mailchimp/SendGrid	Client contact details	Marketing
21.4	Microsoft Word, Excel	Client contact details (contracts), app end user data (results tables from CMS Forms)	Workflow
21.5	Adobe PDF/Adobe Suite	Client contact details (contracts)	Workflow
21.6	Sage Accounting	Client contact details	Accounting
21.7	Microsoft ASP .Net tools	Admin user only – name, email, Aliases, Groups, Security Settings, Admin Roles	Developer tool
21.8	Microsoft SQL Server	Admin user only – name, email, Aliases, Groups, Security Settings, Admin Roles	Developer tool

21.9	Plesk	All CMS data	Web hosting
21.10	Dropbox/WD Local Cloud Drive	Customer Theme data, Backups of their data, Documents, built apps storage, development storage	System back up

22. **Data Security – Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

a. All emails containing personal data must be marked “confidential”;
b. Personal data must be transmitted over secure networks only;
c. Personal data may not be transmitted over an unsecured wireless network if there is a wired alternative that is reasonably practicable;
d. Personal data contained in emails, whether sent or received, should be deleted as soon as the information contained in them is no longer required for the task at hand.
e. Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient; and
f. All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

23. **Data Security – Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

a. All electronic copies of personal data should be stored securely using passwords and where necessary data encryption;
b. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
c. All personal data stored electronically should be backed up. All backups should be encrypted;
d. Personal data should not be transferred to any device personally belonging to an employee but if this is unavoidable the employee concerned must treat it with the same level of care, attention and compliance with all other aspects of this Policy as they would if the data was held on a Company device.
e. Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR.

24. **Data Security – Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

25. **Data Security – Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

a. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from their manager or a director;
b. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of a director;
c. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

d. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and
e. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Marketing Manager to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the SendGrid.

26. **Data Security – IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

a. All passwords used to protect personal data should be changed regularly and should not be words or phrases that can be easily guessed or otherwise compromised.
b. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff and contractors do not have access to passwords;
c. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Each individual shall be responsible for installing any and all security-related updates promptly after it is released and/or when they are requested to do so by the Head of IT;
d. No software may be installed on any Company-owned computer or device without the prior approval of the Director of Technical Services.
e. A log will be maintained of all Company-owned devices and personal devices used by any employees, agents, contractors, or other parties working on behalf of the Company and appropriate device settings activated such that the Company can remotely delete data from any devices lost or stolen.

27. **Organisational Measures**

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
b. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
c. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
e. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
f. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g. All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;
h. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
i. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
j. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data

are held to the same conditions as those relevant employees of the Company arising out of this Policy and the GDPR; and

k. Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28. **Transferring Personal Data to a Country Outside the EEA**

a. The Company will take all reasonable measures to ensure data remains inside the EEA region but it may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA. For example, internet networks are designed to transmit email messages by the most efficient route available at the time without regard to geography.
b. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
    1. The Client or an app end user is based in a country outside the EEA.
    2. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
    3. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
    4. The transfer is made with the informed consent of the relevant data subject(s);
    5. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
    6. The transfer is necessary for important public interest reasons;
    7. The transfer is necessary for the conduct of legal claims;
    8. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
    9. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

29. **Data Breach Notification**

a. All personal data breaches must be reported immediately to the Company's Data Protection Officer.
b. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
c. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
d. Data breach notifications shall include the following information:
    1. The categories and approximate number of data subjects concerned;
    2. The categories and approximate number of personal data records concerned;
    3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);

4. The likely consequences of the breach;
5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

30. **Implementation of Policy**

This Policy shall be deemed effective as of 06 April 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

1. What information is available to monitor who is accessing my data?

There are three types of users identified in the system – teachers, students and parents. Teachers and parents are able to see when their registered students last logged into the system and for how long from the activity report.

2. Do you sub-contract to other data processors and will you ask us before, if you do use a sub-processor?

We do not use sub-processors as part of our processing service to our customers. As per Article 28 (2) of the GDPR, we confirm that we shall not use a sub processor without prior written consent from the controller.

3. How does JellyJames ensure secure storage of the data I hold?

Protecting data to and from your browser (in transit)
Our software is only available on the application server that is separate from the website. We have carried out penetration tests to secure the servers from any un-authorised access.

4. Data Centre security

JellyJames owns and runs its own dedicated servers out of a data centres located by TSOhost in the UK. They are also responsible for controlling the secure firewall between the external and internal network on our instruction only.
Physical access to the data centre is heavily restricted, and is controlled both at the perimeter and at the building by trained professional security staff. The data centre sites are monitored by CCTV 24 hours a day and are also monitored by other additional intrusion prevention systems. Access is only granted to those who have been authorised in advance or are accompanied by an authorised person. Such access would be subject to identification checks prior to entry. Biometrics are used to ascertain the identity of authorised person/s, and access to the data centre floor is controlled by an anti-piggyback door system that ensures only one person gains access at a time. Once through, authorised users are then required to provide pin access to the data centre floor and key access to their specified server rack. Individual server access is restricted by lockable face plates on the front of each server.
Our data centres maintain ISO27001 and PCI compliance. Details of this can be found here:
https://www.tsohost.com/data-centre-and-network

5. Access control

Access to Dynamo Maths, MySchoolTests and MultistepMaths is provisioned by a single main system administrator account which is specified by the school. Every account after that is provisioned by the school. In the unlikely event that you have issues and you have contacted us, we may ask for temporary access to your account whilst we make our investigations.
Access to the back end of our software is restricted to certain employees who require this to maintain the servers and assist with escalated queries from customers. All employees that are given access to the back end, are subject to an enhanced contract of confidentiality and are governed by additional policies and procedures. When employees with access to the backend are required by schools to access their data, they access it in a raw format to effectively troubleshoot the issue. It is important to remember that this data will only be accessed at the request of the school. It is also important to remember that we cannot give passwords out of

user.

6. Internal controls

Internally, we have a policy of restricting access globally and then providing access to only the areas that each person is required to access in order to perform their role. This helps control and limit our surface area and track how data moves through the company and audit this effectively. Every employee's role is policy driven in the company, giving guidance on how data should be protected, distributed and connected.

7. Backup and availability

Our server setup offers replication, failover and backup between data centres. Our backups occur every day. We have a system of monitoring our servers 24 hours a day which notifies us of potential issues that may exist on the platform. We have staff on call who are tasked with resolving issues as soon as possible.
8. Updates and external review
Our software is constantly being modified and updated to resolve issues that we may have discovered. However, these updates are limited to going live every month.
Firmware and server updates are applied TSOhost on a 2-weekly basis, though we do monitor the updates coming through and if a particular update represents as a high risk, we seek to get this installed as soon as possible. Most updates occur overnight and any servers that require restarting are done so during this time.
Our system is externally reviewed when required. We do internal penetration testing with each release and assess the outcome to decide whether we should go live. If we make a change to significant high-risk areas of the system (such as authentication, encryption etc.), we will push forward an externally administered penetration test earlier to assess whether the release is eligible for the live environment.

9. Sensitive data

All the data entered in by school administrator or parent and we do not store any images of children. Schools are free to change their student details to fit their privacy requirements. We do not attempt to modify any data entered by schools or parents.

10. What is JellyJames data deletion and retention policy, and associated timescale?

Our current retention policy is sympathetic of school's busyness and seeks to support them in the event they cancel their service. As it stands, after the contract end date has passed, we allow users to access data if required for 30 days and download upon request.

11. What is JellyJames doing to prepare for GDPR?

We are already well placed for the GDPR to come into effect as our business processes and company ethos complement the requirements of the GDPR. That said, because we are a small company, there are some things we need to bring into place in order to consider ourselves fully compliant. These include:

- Updating our processes and privacy policy to ensure our compliance in respect of the data we hold about our users
- Updating our notification and email messages with Article 6 clauses to maintain transparency with customers how we have achieved our goal of establishing lawful processing as required under the GDPR.

12. How do we monitor our networks?

We use a range TSOhost datacentre systems to monitor our networks in the data centre. Firstly, we use enterprise grade firewalls to protect our networks and check the information that flows in and out. This is our greatest protector blocks all but the essential traffic from accessing our systems.

13. Will we only process data in accordance with my instructions, and is there a written contract?

We will only process your personal data according to your instructions as Data Controller in accordance with our Terms and Privacy Policy.

14. Will my data be shared with third parties?

We will never disclose personal data with third parties without your permission and this includes using sub-processors to process our data in full or in part. However, we do use the email addresses of authorised users (not parents) in the system to send information to which we have established lawful processing under Article 6 b, c and d. This can include system maintenance notifications, new versions released or important information regarding our system changes that are influenced by changes at government level. The system we use to send these emails means this email address information is transferred from our hosting to the email system. This is necessary in order to allow our customers to opt out of these communications.

15. How is my data protected from accidental destruction?

We backup our systems every day and the data will be retrieved from the backup copy kept in the secure data centre.

16. How are users I invite protected from unauthorised use of their log-in

When a user is invited to access our software, the email they receive contains details of the person and school that is requesting they join. They are provided with a link which when they click on, sends them to a page where they set a password. At present, that password is required to have 3 of the following contained within a minimum length 10-character password:

- Uppercase
- Lowercase
- Special character
- Number

To help reduce the chance of access to unattended machines left logged in, we also insist (unless the option is changed at log in), that an inactive session only remain open for 30 minutes. After this time, it logs out and requires the user to log in once more. We suggest that passwords are updated regularly by users and never shared.

17. In what countries does Capsule process your data and what safeguards are in place at these locations?

Data exists only in the U.K and does not leave the U.K at any point. We would, if it occurred, seeks permissions from the individual schools before making a transfer, should the need arise. In the event that this happened, your data would only be transferred to a country that the European Commission has determined provides an adequate level of protection, or to service providers who have an agreement with us committing to the Model Contract Clauses defined by the European Commission, or certified under the Privacy Shield. Further information on Model Contract Clauses can be found in the UK Information Commissioner's Office (ICO) guide.

18. How will you notify us if a breach occurs?

In the unlikely event that we detect a breach or a breach occurs, we shall make contact with the School administrator or parent (or other legally responsible person in the setting), within 72 hours. Method of communication will be by telephone or by email, dependent upon the severity of the breach.

19. How can I get a copy of the data I store on my account and will it be in a format I can use?

Student data is able to be exported by school administrator or parent from the system using 3 export methods. The first method is the student list and their login details by school administrator, student reports exported by school administrators and certificates printed by school administrators.

20. What service levels do you provide and will the capacity allow for demand from other customers or will it impact the quality of my service?

We operate at a 99.9% uptime guarantee. We constantly monitor our servers within the datacentre and their load to see how it is increasing over time. When we deem it necessary, we introduce new servers in advance of there being a capacity problem. We also look at ways of speeding up our system by enhancing our calls and procedures.

21. What will we do in the event of data breach?

A breach can occur in many ways. It seems to be a misunderstanding that the only way data can be breached is by having it forcibly taken from you or one of your systems, however this is not always the case. Data can be breached in a multitude of ways. One of the simplest forms is by an email being forwarded to the wrong person (depending on content of course). We may also be informed by a concerned party that data has been breached or discover through one of our monitoring systems that we may have been hacked.
As soon as a data breach is detected or a data breach is logged with us and subsequently found to be true, we shall enact our requirements under Article 33 and assist you (the Controller) in your requirements to Article 34 in communicating with the data subject if required. Above this, we will also assist the controller in dealing with any media attention statements that may be required dependent upon the severity of the data breach.

22. How can I get a copy of the data I store on my account and will it be in a format I can use?

Student data is able to be exported by school administrators only to the CSV files.

23. What service levels do you provide and will the capacity allow for demand from other customers or will it impact the quality of my service?

We operate at a 99.9% uptime guarantee however we have exceeded this over the last 2 years. We constantly monitor our servers and their load to see how it is increasing over time. When we deem it necessary, we introduce new servers in advance of there being a capacity problem. We also look at ways of speeding up our system by enhancing our calls and procedures.
Our excess capacity as standard reduces the risk of high user usage affecting customers quality of service.

24. What will we do in the event of data breach?

A breach can occur in many ways. It seems to be a misunderstanding that the only way data can be breached is by having it forcibly taken from you or one of your systems, however this is not always the case. Data can be breached in a multitude of ways. One of the simplest forms is by an email being forwarded to the wrong person (depending on content of course). We may also be informed by a concerned party that data has been breached or discover through one of our monitoring systems that we may have been hacked.
As soon as a data breach is detected or a data breach is logged with us and subsequently found to be true, we shall enact our requirements under Article 33 and assist you (the Controller) in your requirements to Article 34 in communicating with the data subject if required. Above this, we will also assist the controller in dealing with any media attention statements that may be required dependent upon the severity of the data breach.

25. What is the timescale you have to notify us of a breach?

In Article 33 (Notification of a personal data breach to the supervisory authority) of the GDPR. Section 1 states:

1) *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

   This means, you as a school have 72 hours from being **made aware** by us to notify the data subject/s of the breach in accordance with the stipulation of Article 33 Section 3, at the very least. This 72

hours does not run from the time the breach actually happened, rather from when you were notified that a breach had occurred. As processors, we are bound by Article 33 Section 2 which states:

2) *The processor shall notify the controller without undue delay after becoming aware of a personal data breach.*

Whilst the above does not specify a time frame from the processors perspective, if we look at Article 34 Section 1 it says:

1) *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

This would then indicate that their definition of undue delay is a maximum of 72 hours (the requirements of Article 33 Section 3 can be disseminated over time as per Article 33 Section 4, again without undue delay), so as soon as we are aware of a data breach, this is the period of time that we have to contact you to notify you of a breach of the data upon which you are the controller and we are the processors.

Just to reiterate, this timer runs from the point you as data controllers are made aware (by us telling you) and a separate timer when we as data processors are made aware (by us discovering the breach through monitoring systems, or by internal employees), it does not run from the time the breach actually occurred.

JellyJames Online Software Access and Cookies Policy

1. **Online Software Access**

JellyJames online application websites do not store or capture personal information, but for administration purposes, it merely logs the user's IP address, which is automatically recognised by the web server and access reporting.

2. **Cookies Policy**

When we provide services, we want to make them easy, useful and reliable. Where services are delivered on the internet, this sometimes involves placing small amounts of information on your device, for example, computer or mobile phone. These include small files known as cookies. They cannot be used to identify you personally.

These pieces of information are used to improve services for you through, for example:

a. enabling a service to recognise your device so you don't have to give the same information several times during one task;
b. recognising that you may already have given a username and password so you don't need to do it for every web page requested;
c. measuring how many people are using services, so they can be made easier to use and there's enough capacity to ensure they are fast.

You can manage these small files yourself and learn more about them with this advice from Directgov: https://www.gov.uk/help/cookies

3. **Our use of Cookies**

We use analytics cookies primarily to monitor which browser types and operating systems people are using. This enables us to create a site that works with many different browsers, improving the service we can offer.

More details on these cookies can be found on the Google Code pages (https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage?csw=1#cookiesSet). You can disable these cookies so we can't record this information. Cookie for recording the enabling/disabling of cookies. This cookie records whether you wish to enable or disable cookies. If you elect to disable the above cookies this cookie is used to record your decision so you are not prompted each time you visit this site.

Our applications websites will not function without this cookie. For further details on the cookies set by Microsoft ASP.NET, please refer to the Microsoft website. Details...(https://support.microsoft.com/en-gb/help/899918).

We will not use cookies to collect personally identifiable information about you.

However, if you wish to restrict or block the cookies which are set by our websites, or indeed any other website, you can do this through your browser settings.

The Help function within your browser should tell you how. Alternatively, you may wish to visit www.aboutcookies.org which contains comprehensive information on how to do this on a wide variety of browsers.

You will also find details on how to delete cookies from your machine as well as more general information about cookies.

Please be aware that restricting cookies may impact on the functionality of our website. If you wish to view your cookie code, just click on a cookie to open it.

You'll see a short string of text and numbers. The numbers are your identification card, which can only be seen by the server that gave you the cookie.

For information on how to do this on the browser of your mobile phone, you will need to refer to your handset manual. To opt out of third-parties collecting any data regarding your interaction on our website, please refer to their websites for further information.