

UniqueSchools

Data Protection Policies & Procedures

Contents

1. **US** Data Security
2. **US** Service Provider Confidentiality/
Data Processing Agreement
3. **US** Data Protection Policy
4. **US** Data Privacy Impact Assessment
5. **US** Group Business Structure

Welcome to our Data Protection Policies & Procedures. The purpose of this document is to set out in plain language all the information our customers, staff and data subjects need to know regarding Unique Schools processes, procedures and obligations on data protection.

Data Processing Agreement

A copy of our standard DPA is included here for reference. Each client who is availing of our Digital Communications, Administration, Digital Attendance Form and App system will receive a personalised, signed copy which must be countersigned and returned to Unique Schools. We cannot process any data until this document is in place.

Our processes and procedures will change from time to time in line with best practise and the evolving legal landscape. This document will be updated to reflect these changes and shared with our clients/employees.

Data Breach

All data breaches must be immediately reported to James Mc Manus 087 254 2559, james@uniqueschools.ie. and then to your point of contact in Unique Schools.

If you need any further clarification on any aspect of this document please direct your enquiry to james@uniqueschools.ie.

US **Data** **Security**

US Data Security

Your data is safe

Security, Protection and the Integrity of customer's data is our highest concern. In doing so we have partnered with Amazon to safely store and manage your school's data.

ISO 27001 Certification:

Each Worldwide Amazon Data Center is ISO 27001 certified.

Encryption at Rest:

We encrypt your school's data using AES-256 bit encryption, the same standard used by banks to secure customer data.

Encryption in Transit:

We utilise Secure Socket Layer (SSL) for data transfer, which establishes a secure connection protected by AES-256 bit encryption.

User Management:

Add and remove users as your staff change.

- **Data privacy** We take the privacy of users and schools very seriously and therefore comply with all data protection laws in the European Union i.e. the GDPR.
- **Hosting** Our Software Programme is deployed via Amazon Web Services®.
- **ISO 27001 Certification** Each Worldwide Amazon® Data Center is ISO 27001 certified. ISO 27001 is an international standard on how to implement, monitor, maintain, and continually improve the Information Security Management System (ISMS) for data centres.
- **Encryption** At rest / in transit ensuring that your data is secured and can be safely accessed if required.
- **Data integrity and availability** 99.99% uptime & availability, with data automatically replicated in a second data center.
- **Data Restore** Up to 30 days Point in Time restore is designed for recovering a database from a recent backup after accidental data corruption or deletion.
- **Backups** Your data is backed up nightly ensuring data is never lost.
- **Secure Log in** Each user is required to have a username and password to access data on the software application.
- **User management** Add and remove users as your staff changes.
- **Communication** All communications with the server is performed over HTTPS, thus safeguarding your organisations communications.

Your school's data is always hosted in Europe



Our Commitment to Schools

We will establish a Data Processing Agreement / Standard Contractual Clause with your school on signing up to our service as per the requirements of the GDPR.

- We will only process personal data on documented instructions from you the controller;
- We will ensure that persons authorised to process the personal data in our business have committed themselves to confidentiality;
- We will take all measures pursuant to Article 32 on the security of processing;
- We will respect the conditions for enlisting another processor or sub-processor;
- We will assist the school by appropriate

technical and organisational measures for the fulfilment of the school's obligation to respond to requests to exercise data subjects' rights;

- We will assist the school in complying with the obligations in Articles 32–36 (security, data protection impact assessments and breach notification), considering the nature of the processing;
- We, on written instruction from the school, will delete or return all personal data to the school after the end of the of the services; and
- Make available to the school all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

US

Service Provider Confidentiality/ Data Processing Agreement

US Service Provider Confidentiality / Data Processing Agreement

THIS AGREEMENT is dated DATE OF CONTRACT HERE and made between:

- (1) SCHOOL NAME & CONTACT DETAILS HERE
- and
- (2) Unique School Communications Limited, T/A Unique Schools company registration number 481909, Unit 38 Block 4, Northwood Crescent, Santry, Dublin 9

RECITALS

- A. In connection with a current or proposed Service between the School and the Service Provider, whereby the Service Provider is supplying, or proposes to supply, goods or services (the **Service**) to the School, the School may directly make available to the Service Provider from time to time the *Information* (as defined below), or the Service Provider or its servants, employees, agents, affiliates, subsidiaries or sub- contractors may indirectly acquire or have access to the *Information* by virtue of the Service.
- B. It is intended that this Agreement will govern the terms and conditions applying to the Service Provider's use of the *Information* and other related matters.

NOW IT IS HEREBY AGREED by and between the parties hereto as follows:

1 Definitions: In this Agreement, unless the context otherwise requires:

Contact Data means personal data limited to the business contact details of any employee of the School who will communicate with Service Provider personnel regarding the *Service*;

Data Breach has the same meaning as "personal data breach" as set forth in Article 4 of the GDPR;

Data Controller has the meaning given to that term in Article 4 of the GDPR;

Data Processor or Processor has the meaning given to that term in Article 4 of the GDPR;

Data Subject has the meaning given to this term in the GDPR;

Delete for the purposes of this agreement means removing all *Information* which is electronically held in such a way that it can never be retrieved from the device on which it is held;

FOIA 2014 means the Freedom of Information Act 2014 and any amendments to or replacements thereof, including by means of directly effective EU Regulation;

GDPR means the EU General Data Protection Regulation, Regulation (EU) 2016/679, the effective date of which is 25th May 2018;

Information means all information, (irrespective of the format, paper, electronic or otherwise) that is provided to the Service Provider by or on behalf of School in connection with the *Service*. *Information* may include *Personal Data* concerning School, students and staff;

Personal Data has the meaning given to that term in Article 4 of the GDPR, and relates only to personal

data, or any part of such personal data, of which the School is the Data Controller or joint Data Controller and in relation to which the Service Provider is providing the Service, and includes Sensitive Personal Data and Special Categories of Data;

Processing and Process has the meaning given to those terms in Article 4 of the GDPR;

Pseudonymisation, Pseudonymised and like words, have the meaning given to those terms (when effective) in Article 4 of the GDPR;

Sensitive Personal Data has the meaning given to this term in the GDPR;

Special Categories of Data has the meaning given to this term and/or such Personal Data as referred to in Article 9(1) and/or Article 10 of the GDPR.

Standard Contractual Clauses means the Standard Contractual Clauses pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to Processors established in third countries under the Directive set forth in Exhibit 1 to and forming part of this agreement.

Any reference to **third party** in this Agreement includes, for the avoidance of doubt, subcontractors.

Obligations of the Service Provider:

In consideration of the School directly making the *Information* available to the Service Provider, or the Service Provider otherwise acquiring the *Information*, and in consideration of the award of the Contract, the Service Provider shall:

- 1.1 Manage and Process any *Information* which they acquire from the School in accordance with the documented instructions of the School as set out in this Agreement and the obligations of the *GDPR* in so far as these obligations apply to a *Data Processor*, including with regard to transfers of *Personal Data* to a third country or an international organisation, unless required to do so by European Union or Irish law to which the Service Provider is subject; in such a case, the Service Provider shall inform the School of that legal requirement before *Processing*, unless that law prohibits such information on important grounds of public interest;
- 1.2 Maintain secret and confidential all *Information* furnished to it or otherwise acquired by its servants, employees, agents, affiliates, subsidiaries or sub-contractors save and to the extent that such *Information* has been made available to the public by the School or by any third party lawfully in possession thereof and entitled to make such disclosure without restriction;
- 1.3 Take appropriate measures to ensure the reliability and confidentiality of the Service Providers servants, employees, agents, affiliates, subsidiaries or sub-contractors who have access to the *Information*; The Service Provider must be in a position to provide the School with a named list of their servants, employees, agents, affiliates, subsidiaries or sub-contractors authorised to have access to *Information*.
- 1.4 Not disclose *Information* to any of the Service Provider's servants, employees, agents, affiliates, subsidiaries or sub-contractors unless and only to the extent that such persons need to know such *Information* for the purposes of providing services in connection with the Service, and provided that such person has been made aware of the restrictions in this Agreement on the disclosure of the *Information* and has agreed in writing to comply with such restrictions or materially similar restrictions;
- 1.5 Not disclose any *Information* to any third party without the prior written consent of the School unless the Service Provider is legally required to do so (see Clause 3.0 of this Agreement); in this regard both parties are fully aware of the company and business structure of Unique School Communications Limited and agree to the ongoing IT services, support, data processing, testing and system development, provided by Unique School App India LLP a company 80% owned and controlled by James Mc Manus whose sole customer is Unique School Communications Limited;
- 1.6 Not engage any third party to process the *Information* or any part thereof on its behalf without the prior written consent of the School; in this regard both parties are fully aware of the company and business structure of Unique School Communications Limited and the ongoing IT services, support, data

processing, testing and system development, provided by Unique School App India LLP a company 80% owned and controlled by James Mc Manus whose sole customer is Unique School Communications Limited; Should such consent be given, then the obligations of the Service Provider as set out in Clause 2 of this Agreement shall be imposed on that third party by way of a separate written agreement between the Service Provider and the third party, which agreement will terminate automatically upon termination of this Agreement for any reason. In the event that the third party fails to fulfil its obligations set out in Clause 2 of this Agreement, the Service Provider shall remain fully liable to the School for the performance by the third party of those obligations;

- 1.7 Not use the *Information* directly or indirectly for any purpose other than in connection with the provision of services to the School regarding the Service;
- 1.8 Not reverse engineer, de-compile or disassemble *Information* or attempt to use the *Information* in any form other than machine readable object code, or allow a third party to do any of the above;
- 1.9 Only use the *Information* solely for the purposes of fulfilling the requirements of the Service.
- 1.10 Take the necessary precautions for the prevention of unauthorised access to, unauthorised disclosure of or other unauthorised processing of the *Information* and in particular:
 - 1.10.1 Keep all *Information* obtained from the School or otherwise relating to the Service separate from all documents and other records of the Service Provider. The School accepts that this requirement would be achieved by the Service Provider through logical electronic separation using role based access controls;
 - 1.10.2 Only make such copies of the *Information* as are necessary for the provision of services to the School regarding the Service; and
 - 1.10.3 Ensure that any notices related to the confidentiality or privacy of the *Information* provided by the School are not removed or altered; and
 - 1.10.4 Have all necessary access controls in place to include authentication and authorisation for access to *Information* to ensure its security and confidentiality; and
 - 1.10.5 Have all necessary systems in place to ensure the ongoing confidentiality, integrity, availability and resilience of *Processing* systems and services; and
 - 1.10.6 Have the ability to restore the availability and access to the *Information* in a timely manner in the event of a physical or technical incident; and
 - 1.10.7 Have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the *Processing* of the *Information*;
- 1.11 Ensure, upon termination or the completion of this Agreement, that all documents, data, other records or tangible objects containing or representing *Information* which have been disclosed by the School to the Service Provider ("**Information Records**"), and all copies thereof which are in the possession of the Service Provider and their subcontractors, shall at the written request and election of the School, be returned to the School or securely *Deleted*. Without prejudice to the generality of the foregoing:
 - 1.11.1 Where the School has requested that the Service Provider return *Information Records*, the *Information Records* shall be returned from the Service Provider to the School in a commonly used electronic format;
 - 1.11.2 Where the School has requested that the Service Provider securely *Delete Information*, the Service Provider shall ensure the *Information* is permanently *Deleted* from any of the Service Providers systems or devices which were used to store the *Information* and from those of third parties to whom the Service Provider has disclosed and/or permitted access to the *Information* or *Information Records*;
 - 1.11.3 Where the Service Provider is required for legal or regulatory compliance to retain a copy of any

Information, the Service Provider shall provide the School in writing with full details of any *Information* they are proposing to retain and the details of the legal and regulatory obligations governing this action.

- 1.11.4 Without prejudice to the obligations at Clause 2.13.3 above, in circumstances where European Union or Irish law requires the Service Provider to retain any *Personal Data* which the School has shared with the Service Provider, the Service Provider shall provide the School in writing with full details of any *Personal Data* they are legally required to retain and the details of the European Union or Irish legal obligations governing this action, and ensure the *Personal Data* retained by them is anonymised or *Pseudonymised* by them to the School's satisfaction and in a manner and to a standard which is satisfactory under European Union law (including, without limitation, the *GDPR*);
- 1.12 Implement appropriate technical and organisational controls in accordance with Article 32 of the *GDPR*, to keep the *Information* secure and to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the *Information* transmitted, stored or otherwise processed by the Service Provider;
- 1.13 Provide reasonable assistance to the School relating to its compliance with the provisions of Articles 33 to 36 of the *GDPR* and/or any guidance issued by the Irish Data Protection Commissioner;
- 1.14 Notify the School without undue delay, after they or (as applicable) their subcontractors become aware of a *Data Breach*. In the event of a *Data Breach*, the Service Provider will:
 - (a) investigate the *Data Breach*, (b) provide the School with all the relevant details surrounding the *Data Breach*, (c) provide the School with details of the measures taken or proposed to be taken by the Service Provider to mitigate the effects and to minimise any damage resulting from the *Data Breach*, and (d) assist the School in fulfilling its obligation to notify the relevant supervisory authority and *Data Subjects* of a *Data Breach* in accordance with Articles 33 and 34 of the *GDPR*;
- 1.15 Taking into account the nature of the processing, assist the School by appropriate technical and organisational measures, insofar as this is possible, to enable the School to fulfil its obligations to respond to requests from Data Subjects and Chapter III of the *GDPR*, (including the rights of access to, rectification of and erasure of their *Personal Data*), and shall promptly comply with any request from the School to amend, transfer or *Delete* such *Personal Data*.
- 1.16 For the purposes of Freedom of Information / transparency obligations placed upon the School (by *FOIA 2014* or otherwise):
 - 1.16.1 Procure that it and its servants, employees, agents, subsidiaries or sub-contractors shall assist the School, at no additional charge and within such timescales as the School may reasonably specify, in meeting any requests for *Information* which are made to the School under the *FOIA 2014*, such assistance to include (but not be limited to) the provision of a copy of the requested *Information*.
 - 1.16.2 Notwithstanding anything to the contrary in this Agreement, if the School receives a request for *Information* pursuant to the *FOIA 2014*, the School shall be entitled to disclose all *Information* (in whatever form) as is necessary to comply with the *FOIA 2014*.
 - 1.16.3 If, at the request of the Service Provider, the School seeks to withhold *Information* protected by this Agreement and a competent authority determines, or the parties subsequently agree, that the *Information* is not exempt, then the Service Provider shall reimburse the School for all costs (including but not limited to legal costs) incurred by the School in seeking to withhold such *Information* from a request under the *FOIA 2014*.
 - 1.16.4 Not (and shall procure that its servants, employees, agents, subsidiaries or sub- contractors do not) respond directly to a request for *Information* under the *FOIA 2014* unless expressly authorised to do so by the School.
- 1.17 Ensure the security of *Information* stored on all fixed and mobile devices, including mobile devices, desktop computers, servers and mobile computer devices (i.e. laptops, notes, tablets, personal data assistants, Blackberry enabled devices, iPads, iPhones and other smart type devices etc) and removal

- storage devices (i.e. CD, DVD, portable hard drives, Diskettes, ZIP disks, Magnetic tapes etc).
- 1.18 Ensure the security of the *Information* in transit (including by way of electronic transit/ transit by way of electronic communication). Where it is necessary to transfer the *Information*, the Service Provider must take all necessary precautions to ensure the security of the *Information* before, during and after transit.
- 1.19 In relation to transfers of *Information* outside of the Republic of Ireland.
- 1.19.1 Where the School has consented to the transfer of *Information* outside the Republic of Ireland, the Service Provider may only transfer *Information* to a legal entity located in:
- 1.19.1.1 A country within the European Economic Area;
- 1.19.1.2 A country outside the European Economic Area but approved for this purpose by the EU Commission pursuant to Article 45(3) of the *GDPR*;
- 1.19.1.3 A country outside the European Economic Area but subject to the execution by the School, the Service Provider and the transferee of standard data protection clauses adopted by the EU Commission in accordance with the examination procedure referred to in Article 93(2) of the *GDPR*, as provided for in Article 46 of the *GDPR*;
- 1.19.1.4 A country outside the European Economic Area but where the transferee of the *Information* is a parent or subsidiary company of the Service Provider, provided that the Service Provider and that parent or subsidiary company have adopted Binding Corporate Rules which have been approved by the relevant national Data Protection Authority under Article 47 of the *GDPR*;
- 1.19.1.5 The United States of America only when the *Information* transferee has agreed in writing to be bound by the European Commission's Implementing Decision (EU) 2016/1250 of 12th July 2016 (EU-US Privacy Shield).
- 1.20 Make available to the School all information necessary to demonstrate the Service Providers compliance with the obligations laid down in Article 28 of the *GDPR* and allow for and contribute to audits, including inspections, conducted by the School or another auditor mandated by the School. The Service Provider and the School agree to negotiate in good faith the scope and implementation details of this provision at the time the School decides to exercise its rights under this provision.
- 2 Disclosure Required by Law:** In the event that the Service Provider is legally required to disclose any of the *Information* to a third party, the Service Provider undertakes to notify the School of such requirement prior to any disclosure and, unless prohibited by law, to supply the School with copies of all communications between the Service Provider and any third party to which such disclosure is made. The Service Provider must co-operate with the School in bringing any legal or other proceedings to challenge the validity of the requirement to disclose *Information*.
- 3 Breach of Agreement:** The Service Provider hereby indemnifies and agrees to keep indemnified the School against any costs, expenses, damages, harm or loss suffered or incurred by reason of any disclosure of the *Information* in breach of the terms and conditions of this Agreement and shall account to the School for any moneys received by the Service Provider directly or indirectly arising out of the disclosure or use of any of the *Information* in breach of the terms and conditions of this Agreement.
- 4 No Warranty:** Nothing in this Agreement shall constitute a warranty by the School as to the accuracy of any of the *Information*, and the School will not be liable to the Service Provider or to any other party to which any of the *Information* may be disclosed for any loss or damage howsoever caused, arising directly or indirectly out of the inaccuracy of any of the *Information*.
- 5 No Licence:** The Service Provider acknowledges that the *Information* is of a special and unique character and that the *Information* and any patent, copyright or other intellectual property rights of whatever nature attaching thereto are and will remain the property of the School and nothing in this Agreement will be construed as giving the Service Provider a licence in respect of such patent, copyright or other intellectual property rights.

- 6 Survival of Obligations:** The non-disclosure obligations of this Agreement will survive and continue and will bind the Service Provider's legal representatives, successors and assigns notwithstanding that the Service may not be actually implemented by the parties.
- 7 Waiver:** The rights of the School under this Agreement will not be prejudiced or restricted by any indulgence or forbearance extended to the Service Provider or other parties, and no waiver by the School in respect of any breach of the terms of this Agreement will operate as a waiver in respect of any subsequent breach.
- 8 Variation:** This Agreement may not be released, discharged, supplemented, amended, varied or modified in any manner except by an instrument in writing signed by a duly authorised officer or representative of each of the parties hereto.
- 9 Notice:** Any notice or other communication given or made under this Agreement shall be in writing and may be sent by email, delivered to the relevant party, or sent by pre-paid registered post airmail or fax to the address of that party specified in this Agreement or to that party's fax number thereat or such other address or number as may be notified hereunder by that party from time to time for this purpose and will be effective notwithstanding any change of address or fax number not so notified. Unless the contrary is proved, each such notice or communication will be deemed to have been given or made and delivered, if by email upon delivery, if by post 48 hours after posting, if by delivery when left at the relevant address or, if by fax upon transmission, subject to the correct code or fax number being received on the transmission report.
- 10 Severance:** If any provision of this agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions of this agreement will remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision will apply with whatever modification is necessary to make it valid, enforceable or legal.
- 11 Governing Law:** This Agreement will be governed by and construed in accordance with the laws of Ireland and the parties hereto hereby irrevocably submit to the exclusive jurisdiction of the courts of Ireland.

Name: Principal Name Here
Position: Principal
Address: School Name & Address here

Other information necessary in order for the contract to be binding (if any):

Signature: _____ Date: 16 November 2020

Name: James McManus on behalf of Unique School Communications Limited, T/A Unique Schools
Position: Managing Director
Address: Unit 38, Block 4, Northwood Crescent, Santry, Dublin 9.

Other information necessary in order for the contract to be binding (if any):

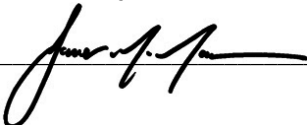
Signature:  _____ Date: 16 November 2020

Exhibit 1
STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation	School Name & Contact Details Here
e-mail:	School Details Here (the data exporter)

And

Name of the data importing organisation:	James McManus on behalf of Unique School Communications Limited, T/A Unique Schools Unit 38, Block 4, Northwood Crescent, Santry, Dublin 9.
Tel.	087 254 2559
e-mail:	james@uniqueschools.ie (the data importer)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1 **Definitions**

For the purposes of the Clauses:

1. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);
2. 'the data exporter' means the controller who transfers the personal data;
3. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
4. 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
5. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
6. 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

(1) Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

1. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
2. that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
5. that it will ensure compliance with the security measures;
6. that, if the transfer involves special categories of data, the data subject has been informed or will be

informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

7. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
8. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
9. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

1. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
2. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
5. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
6. any accidental or unauthorised access; and
7. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
8. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
9. at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
10. to make available to the data subject upon request a copy of the Clauses, or any existing contract for

sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

11. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent; in this regard both parties are fully aware of the company and business structure of Unique School Communications Limited and the ongoing IT services, support, data processing, testing and system development, provided by Unique School App India LLP a company 80% owned and controlled by James Mc Manus whose sole customer is Unique School Communications Limited;
12. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
13. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

-
- (2) Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
4. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or

claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

- a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 **Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9 **Governing law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the Republic of Ireland.

Clause 10 **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11 **Sub-processing**

1. The data importer uses the services of s Unique School App India LLP a company 80% owned and fully controlled by James Mc Manus; Unique School App India LLP are the dedicated IT Services provider for all of Unique Schools Communications Limited ongoing IT services, support, data processing, testing and system development; The data importer shall not subcontract any other of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter; Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (1). Where the sub- processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Ireland.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

-
- (1) This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

On behalf of the data exporter

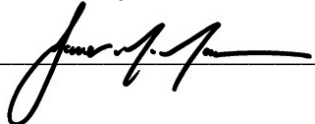
Name: Principal Name Here
Position: Principal
Address: School Name & Address here

Other information necessary in order for the contract to be binding (if any):

Signature: _____ Date: 16 November 2020

Name: James McManus on behalf of Unique School Communications
Limited, T/A Unique Schools
Position: Managing Director
Address: Unit 38, Block 4, Northwood Crescent, Santry, Dublin 9.

Other information necessary in order for the contract to be binding (if any):

Signature:  _____ Date: 16 November 2020

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix:

Data exporter - The data exporter is (please specify briefly your activities relevant to the transfer):

Processing of communications, attendance information, payments, contractual forms, general school information, student and parent data in the general management and running of the school in the normal course of day to day activities.

Data importer - The data importer is (please specify briefly activities relevant to the transfer):

Provision of cloud based IT Services, Communications, Digital Administration systems, processes, Digital attendance form management, updating of schools attendance roll call (where applicable); mobile software application and services for schools.

Ongoing development of the mobile software application including customer account creation, troubleshooting and bug fixing, deployment, and support to customers.

Data subjects - The personal data transferred concern the following categories of data subjects (please specify):

Personal Data relating to students, parents and school administrators of the software.

Categories of data - The personal data transferred concern the following categories of data (please specify):

Name and contact details for students, parents and school administrators of the software. Data relating to P-Pod number, PPS number, Date of Birth & Photographs.

Forms including permission to take photographs, Medical / Health Data Information Form. Attendance Forms & Data

Log data which may include certain source and destination IP addresses, host name, user-ids, URLs, policy names, email addresses, date and time stamps, data volumes, email activity and content;

Special categories of data (if appropriate) - The personal data transferred concern the following special categories of data (please specify):

Health Data is captured using the Medical / Health Data Information Form.

Processing operations - The personal data transferred will be subject to the following basic processing activities (please specify):

Receiving data, accessing, retrieving, and recording same for the purposes of ensuring the digital ecosystem is maintained and fit for purpose for the school including students, parents, teachers. Provision of informational reports and data to allow the school staff perform core duties. Payment processing (where specifically contracted).

Provision of digital attendance form management services, roll/attendance updates based on information received/ requested from app users and/or school data, as specified in the scope of work & annual contract in force at the time of processing.

On behalf of the data exporter

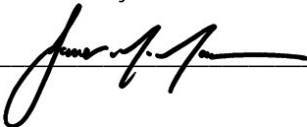
Name: Principal Name Here
Position: Principal
Address: School Name & Address here

Other information necessary in order for the contract to be binding (if any):

Signature: _____ Date: 16 November 2020

Name: James McManus on behalf of Unique School Communications
Limited, T/A Unique Schools
Position: Managing Director
Address: Unit 38, Block 4, Northwood Crescent, Santry, Dublin 9.

Other information necessary in order for the contract to be binding (if any):

Signature:  _____ Date: 16 November 2020

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, The importer shall in relation to the Personal Data implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk.

This includes, but is not limited to:

Access to the information will be restricted to authorised persons on a “need-to-know” basis;

Manual files will be stored in a relevant filing system, located away from public areas in locked cabinets;

Computerised data will be held in secure databases (password protected) with encryption enabled on all databases for data in transit and at rest.

Any information which needs to be disposed of will be done so carefully and thoroughly;

The use of logging mechanisms to verify whether and by whom the data has been accessed, used and/or disclosed.

Data will be protected by strong passwords that are changed regularly and never shared between personnel;

Computers containing personal data will be sited in secure locations;

Data will be backed up frequently;

All computers containing data will be protected by approved security software and a firewall.

On behalf of the data exporter

Name: Principal Name Here
Position: Principal
Address: School Name & Address here

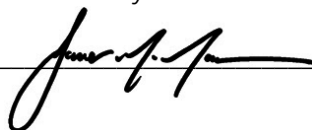
Other information necessary in order for the contract to be binding (if any):

Signature: _____ Date: 16 November 2020

Name: James McManus on behalf of Unique School Communications Limited, T/A Unique Schools
Position: Managing Director
Address: Unit 38, Block 4, Northwood Crescent, Santry, Dublin 9.

Other information necessary in order for the contract to be binding (if any):

Signature: _____ Date: 16 November 2020



US Data Protection Policy



CIRCULATION SHEET

Client	Unique Schools Communications Limited
Project Title	Unique School Communications Limited GDPR Project 2019
Document Title	Data Protection Policy

Revisions				
Rev	Status	Approved By	Office of Origin	Issue Date
R01	Release	Ark Services W: www.arkservices.ie	Cork	November 2019

Circulation			
Name	Organisation	Method	Issue Date
Managing Director	Unique School Communications Limited	Email	November 2019



TABLE OF CONTENTS

1	Introduction	32
2	Scope	32
3	GDPR Compliance Statement	33
4	GDPR Principles	34
4.1	Principle 1: Lawfulness, fairness and transparency	34
4.2	Principle 2: Purpose Limitation	34
4.3	Principle 3: Data Minimisation	34
4.4	Principle 4: Data Accuracy	34
4.5	Principle 5: Storage Limitation	34
4.6	Principle 6: Integrity & Confidentiality	34
4.7	Principle 7: Accountability	34
5	Data Subjects Rights	34
5.1	Rights of Data Subjects	34
5.2	Right of Access (Also known as a Subject Access Request)	35
5.3	Right to Rectification	35
5.4	Right to Erasure	35
5.5	Right to Restrict Processing	35
5.6	Right to Data Portability	35
5.7	Right to Object	36
5.8	Rights in Relation to Automatic Decision Making and Profiling	36
6	Responsibilities	36
6.1	Managing Director	36
6.2	Employees	36
6.2.1	General	36
6.3	Where Unique School Communications Limited is the Data Controller	37
6.4	Where Unique School Communications Limited is the Data Processor (School sharing personal data with us)	37
7	Data Protection Policy	37
7.1	GDPR Awareness	37
7.2	Balance of Rights	37
7.3	Data Protection Impact Assessment	38
7.4	Lawful Processing Criteria	38
7.5	Storage and Use of Personal Data	38
7.5.1	Paper based records	38
7.5.2	Electronic records	38
7.5.3	Use of Personal Data	38
7.5.4	Photographs of Students	39
7.6	Special Categories of Data	39
7.6.1	Children/Students	39

8	Data Processing Map & Retention Policy	39
8.1	Electronic Records	40
8.2	Unique School Communications Limited Employee Personnel Files	44
8.3	Occupational Health Records	48
8.4	Superannuation / Pension / Retirement Records	50
8.5	Financial Records	51
9	Data Protection Communications	52
9.1	The Data Protection Policy	52
9.2	Privacy Notices	52
9.3	Website Privacy Notice	52
9.4	Data Privacy and employees	52
9.5	Communication plan for Privacy Notices	52
10	Third parties	53
10.1	General	53
10.2	Transfers of personal data to non-EEA jurisdictions	53
11	Data Security Breaches	55
11.1	Data Breach Action Plan	55
11.1.1	Identification and Initial Assessment of the Incident	55
11.1.2	Containment and Recovery	55
11.1.3	Risk Assessment	55
11.1.4	Notification	55
11.1.5	Evaluation and Response	56
12	Subject Access Requests (SARs)	56
12.1	Data Subject Rights	56
12.2	Logging Subject Access Requests	56
12.3	Responding to Subject Access Requests	56
12.4	Protecting Third Parties	56
13	Disposal of Personal Data	57
14	Governance Framework	57
14.1	Supervisory authority	57
14.2	Monitoring Compliance	57
14.3	Disciplinary Procedure	57
Appendix		
	Appendix 1: Subject Access Request Form	60
	Appendix 2: Website Privacy Notice	64
	Appendix 3: App Privacy Notice	66
	Appendix 4: Staff Privacy Notice	68
	Appendix 5: Email Privacy Notice	70
	Appendix 6: Subject Access Request Register	71
Acknowledgement of the Data Protection Policy		72

1 Introduction

Unique School Communications Limited is an Irish company based in Glasnevin, Dublin. Our Mobile Apps engage and communicate to students, teachers and parents. They serve as a communication tool between the school and home. Our Apps bring school and college life into the hands of all no matter when or where.

2 Scope

This policy states the commitment of the company to comply with the GDPR as both a Data Controller and Data Processor. It applies to the personally identifiable information of EU residents such as employees, students and staff involved in our programme as well as those attending events & training.

It applies directly to functions of Unique School Communications Limited which collect or process personally identifiable information as part of normal operations. It also applies to external parties who act as Data Processors on behalf of Unique School Communications Limited.

3 GDPR Compliance Statement

Unique School Communications Limited (“the company”) committed to meeting its obligations under the General Data Protection Regulation of 2016 (GDPR). The policy applies to all directors, employees, the schools we work with including students and staff members, their parents/guardians, as well as applicants for positions within the organisation and third party service providers.

Unique School Communications Limited is aware of its responsibilities as both a Data Controller & Data Processor of personal data under GDPR. All employees who will be involved in processing personal information will be informed appropriately as to their responsibilities with respect to GDPR in their day to day work.

We are committed to high standards of data protection, information security & privacy. Unique School Communications Limited respects the privacy of all our end users and is committed to protecting their personal data.

We will safeguard the personal information under our remit and develop a robust data protection regime that is effective, fit for purpose and demonstrates compliance with the GDPR.

Our GDPR Principles:

- We will process all personal data fairly and lawfully;
- We will only process personal data for specified and lawful purposes;
- We will endeavour to hold relevant and accurate personal data, and where practical, we will keep this up to date;
- We will not retain personal data for longer than is necessary;
- We will keep all personal data secure;
- We will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area ('EEA') without adequate protection.

The detailed arrangements for achieving these objectives are set out in the main body of this policy.

Unique School Communications Limited is committed to upholding the standards outlined in this policy. Sufficient authority and resources, both financial and otherwise, will be made available to enable the business to carry out their responsibilities under the GDPR. All employees will be made aware of and have access to this policy.

The Policy will be reviewed annually in light of experience and future developments within the organisation.

Signed:



James McManus
Managing Director
On behalf of Unique School Communications Limited

Date: 27 May 2021

4 GDPR Principles

4.1 Principle 1: Lawfulness, fairness and transparency

Unique School Communications Limited believes in operating our organisation fairly and ethically and this will extend to all personal data held for those purposes. Data Subjects will be informed when data is being collected, and at the same time informed what we will use that data for. We will ensure that appropriate technical and organisational measures are in place to secure that data.

Collection and processing of data will be transparent. Privacy notices relating to the data subject rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

4.2 Principle 2: Purpose Limitation

Personal data collected by Unique School Communications Limited will be processed only for the purpose for which it was collected. In the event that this purpose should change, data subjects will be informed within the 30-day regulatory period and consent sought for the change.

4.3 Principle 3: Data Minimisation

Unique School Communications Limited will collect only the minimum quantity of personal data to carry out a particular task. Where appropriate, potential data subjects will be requested not to provide unwanted or inappropriately sensitive personal information.

4.4 Principle 4: Data Accuracy

Unique School Communications Limited will make every effort to ensure that data subjects' information is accurate and up to date. Unique School Communications Limited will endeavour to ensure via appropriate levels of training that it is transcribed accurately. If it is not possible for subjects to correct their data personally, data can be corrected by contacting Reception.

4.5 Principle 5: Storage Limitation

Unique School Communications Limited will store and retain personal data only while there is a valid and lawful basis to do so. Personal information will be deleted when it is no longer required for the purposes for which it was collected.

Where systems do not allow deletion of all records relating to an individual, records will be anonymised by "hashing" personal information fields with substituted generic text.

4.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed securely i.e. in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. Unique School Communications Limited will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.7 Principle 7: Accountability

Unique School Communications Limited is responsible for and is able to demonstrate compliance with GDPR. This means Unique School Communications Limited will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5 Data Subjects Rights

5.1 Rights of Data Subjects

Unique School Communications Limited recognises the following as the rights of Data Subjects in certain circumstances:

- The right to make Subject Access Requests (SARs);
- The right to have inaccuracies corrected (rectification);
- The right to have information erased (right of erasure);
- The right to restrict the processing of information (restriction);

- The right to be informed on why personal data is processed (notification);
- The right to Data Portability;
- The right to object to processing of personal data (object);
- The right not to be subject to decisions based on automated decision making.

5.2 Right of Access (Also known as a Subject Access Request)

Data Subjects have the Right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information;

Subject Access Requests must be responded to within one month through the Director. See Section 11 for the procedure.

5.3 Right to Rectification

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

Rights to rectification must be responded to within one month. See Section 11 for the procedure.

5.4 Right to Erasure

This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected;
- The processing was based on consent, and the Data Subject has now withdrawn their consent;
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller;
- The data was being unlawfully processed;
- The data must be erased to comply with a legal obligation;

On receipt of this request, we will carry out an assessment of whether the data can be erased without affecting the ability of this company / the client (school) / Department of Education to provide future services to the Data Subject or to meet its statutory obligations.

5.5 Right to Restrict Processing

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified;
- When processing is unlawful, and a Data Subject opposes the use and requests restriction to storage instead;
- When the Data Controller no longer needs the personal data, but the Data Subject requires it for the purpose of, or in the defence of a legal claim.

When this Right is exercised, Unique School Communications Limited will carry out an assessment of whether the data can be restricted without affecting the ability of the company / the client (school) / Department of Education to provide future services to the data subject.

5.6 Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one service provider to another in a safe and secure way in a common data format e.g. pdf file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject;
- Where the processing is based on consent or performance of a contract;
- When processing is carried out by automated means.

5.7 Right to Object

Individuals have the Right to object to processing based on:

- Legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for the purposes of scientific/historical research and statistics.

5.8 Rights in Relation to Automatic Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Right not to be subject to a decision applies when:

- It is based on automated processing;
- It produces legal/significant effects on the individual;
- Is necessary for entering into or performance of a contract or authorised by law;
- Is based on explicit consent;
- Does not have a legal/significant effect on the data subject.

At present, automated processing is not performed.

6 Responsibilities

6.1 Managing Director

- Ensure the policy is communicated & implemented throughout the company;
- Ensure personal data is collected and processed in accordance with this policy;
- Ensure that the basic principles of data protection are explained to employees when commencing work at the company;
- Ensure that there are regular updates to data protection awareness, so that data protection is a “living” process aligned to the organisation’s ethos;
- Periodically check data held regarding accuracy;
- Driving privacy and data protection awareness in the organisation;
- Identifying training needs and arranging for refresher training sessions as needed;
- Taking appropriate preventative actions to mitigate the risk of data breaches arising;
- Spearheading the response to any data breach (following the data breach protocol);
- Due diligence of service providers (data processors / sub processors) prior to any service provider being retained including ensuring appropriate written contracts in place with all service providers;
- Ensure that Record-keeping of data protection items is carried out;
- Periodic reviews of all data protection arrangements are carried out.

6.2 Employees

6.2.1 General

- Adhere to the values and standards set forth in this Policy and comply with relevant procedures. Request clarification if there is uncertainty. Read and sign acknowledgement of this policy;
- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification;
- Keeping Personal Data only as per the Retention Policy to satisfy the permitted uses;
- Ensure any personal data is accurately processed in accordance with this policy;
- Keep the company office clean and tidy;
- Ensure that personal data is not visible to others (e.g. leaving files on desk, computers left logged into);
- Keep personal data out of sight of visitors to the office;
- Diligence and attention-to-detail when entering data on to any work related administrative system;
- Ensuring that passwords for accessing software systems are appropriate i.e. 8-12 characters, mixture of upper case / lower case / numbers and symbols;
- Keep data accurate, complete, and up-to-date;

- Ensuring filing cabinets and the office door is kept locked when not in use;
- Respect access-permission levels, never looking into files/records to which you have no genuine employment reason for accessing, adhering to the principle of “need to know”;
- Immediately notify the Managing Director if anyone attempts to obtain unauthorised access to personal data;

6.3 Where Unique School Communications Limited is the Data Controller

Implement appropriate technical and organisational measures and be able to demonstrate that data processing is performed in accordance with the Regulation; review and update those measures where necessary considering at all times (with regard to the processing of personal data):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;

6.4 Where Unique School Communications Limited is the Data Processor (School sharing personal data with us)

- We will only process personal data on documented instructions from the controller (i.e. the school), including with regards to transfers of data outside the EEA;
- We will ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- We will take all measures pursuant to Article 32 on security of processing;
- We will respect the conditions for enlisting another processor or sub-processor;
- We will assist the controller by appropriate technical and organisational measures for the fulfilment of the controller’s obligation to respond to requests to exercise data subjects’ rights. This may include:
- Pseudonymisation and encryption of data;
- The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- We will assist the controller in complying with the obligations in Articles 32–36 (security, data protection impact assessments and breach notification), considering the nature of the processing;
- We on written instruction from the controller, delete or return all personal data to the controller after the end of the provision of data processing services; and
- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

7 Data Protection Policy

7.1 GDPR Awareness

Unique School Communications Limited will ensure that all employees are aware of GDPR and are trained appropriately to their duties in respect of processing of personal data as per this data protection policy. The training and awareness programme will consist of:

- Briefing to all employees;
- A general email to all employees with the Data Protection Policy;

7.2 Balance of Rights

In processing personal data for the operation of the organisation, we will ensure that we will only use a subject’s data if the subject’s rights do not outweigh our lawful basis in using that data.

The balance will be assessed by first checking that we have a lawful basis for using the data, and then evaluating whether disproportionate financial, reputational or social harm could be caused to the individual through our use of their data. We will achieve this on an ongoing basis via the Data Protection Policy and Record of Processing methods already explained in this policy.

7.3 Data Protection Impact Assessment

Unique School Communications Limited will carry out and record an impact assessment appropriate in scope to the sensitivity of the personal data being processed. This will identify risks to the data subject, to compliance and to the organisation with respect to GDPR principles. This exercise will be repeated as required i.e. when a change in practices causes us to re-evaluate the impact on data privacy.

7.4 Lawful Processing Criteria

Unique School Communications Limited processes personal data in the pursuance of several lawful processing criteria. In all cases we examine the balance of rights with respect to the use of personal data. It is our objective to align our activities with the rights of the data subject, such that our use of their data is beneficial to the data subject and that any inconvenience or risk to the data subject is minimal in comparison with the benefits there from. We have established our lawful processing criteria in the Data Map & Processing Activities in Section 8.

7.5 Storage and Use of Personal Data

The security of personal data is a very important consideration under the GDPR and is taken very seriously at Unique School Communications Limited. Appropriate security measures will be taken by the organisation to protect unauthorised access to this data. A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised employees on a “need-to-know” basis;
- Manual files will be stored in a relevant filing system, located away from public areas in locked cabinets;
- Computerised data will be held in secure databases (password protected);
- Any information which needs to be disposed of will be done so carefully and thoroughly;

7.5.1 Paper based records

Paper based records shall be kept in a secure place where unauthorised people cannot access it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them;
- When not required, the paper or files will be kept in a relevant filing system in a locked secured filing cabinet or;
- Scanned, transferred to and saved on a password protected computer;
- Data will be shredded and disposed of securely.

7.5.2 Electronic records

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees;
- Personal Data will only be stored on equipment supplied by the company i.e. desktop computers / laptops;
- Computers containing personal data will be sited in a secure location;
- Data will be backed up frequently;
- All computers containing data will be protected by approved security software and a firewall.

7.5.3 Use of Personal Data

We will only process data to accomplish specified, explicit, and legitimate purposes. We will not process beyond such purposes unless further processing compatible for original purpose data was collected. We use personal data originating from either the school (our client) or the parent (when registering the app) for purposes including:

- to comply with our contractual obligations with the school;
- provision and continuous development of our software products;
- provision of customer support;
- provision of training and support to the school;
- to promote our legitimate business interests;
- to comply with our legal obligations as limited company;
- to comply with our reporting obligations to various government bodies i.e. CRO, Revenue;
- to provide appropriate training, direction and support to our staff;

7.5.4 Photographs of Students

Our clients maintain databases of photographs from school events held over the years. Using our software application, the school community can take photos of students, teachers, parents etc. for use in school related publications, social media etc. Consent is requested from each end user in the app. Should the parent wish to have his/her child's photograph removed from our database at any time, we will duly comply on receipt of a written request from the school (data controller). Please note that any images/videos published by the school in yearbooks, newsletters, papers etc. up to this date, will remain in place based on previous consent given. No further images/videos will be published after the date of revocation.

7.6 Special Categories of Data

7.6.1 Children/Students

Special categories of particularly sensitive personal information requires higher levels of protection and includes data relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation.

In certain circumstances, under the explicit instruction from our client (school as a data controller) we may have access to this category of data. In those circumstances, Unique School Communications Limited will ensure that every measure is taken to secure and keep this data safe. The data will only be used in conjunction with a specific task and will not be further processed thereafter.

8 Data Processing Map & Retention Policy

Everyone who works for Unique School Communications Limited has a responsibility for ensuring data is collected, stored, and handled appropriately. Each person who has access to personal data must ensure that it is handled and processed in line with this policy and the data protection principles.

Personal Data processed at Unique School Communications Limited is summarised in the Data Map along with our legal justification for processing this data and our Retention Policy for same.

Data maps have been prepared to identify our data processing activities. Employees should refer to the Data Map to ensure that personal is stored correctly as per the policy. This shows what data collected, where it is stored, and how it is used.

Data Protection Policy

8.1 Electronic Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D01 Customer Databases	Restricted	Amazon Web Service.	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://aws.amazon.com/compliance/gdpr-center/ . Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TOWQAA4&status=Active Model Contract Clauses in place for Third Parties accessing data outside the EU.	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Service has Internationally-recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI's Common Cloud Computing Controls Catalogue (C5) and ENS High. Recently, AWS also announced compliance with the CISPE Code of Conduct. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.
D02 Customer / Parent / Student Emails	Restricted	Sendgrid API.	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://sendgrid.com/resource/general/data-protection-regulation-2/ . Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TRkAAG&status=Active	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D03 Customer /Parent /Student Phone Numbers	Restricted	US Database using Plivo API.	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://www.plivo.com/legality/privacy/ Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TvpQAAW&status=Active peid=46	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.
D04 In-app Payments	Restricted	US Database using Stripe API.	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://stripe.com/privacy-center/legal Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt000000TQOUAA4&status=Active	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. No data is saved on the providers servers. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.
D05 In-app Messaging	Restricted	US Database using Google Firebase API.	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://firebase.google.com/support/privacy Privacy Shield: https://www.privacyshield.gov/participant?id=a2zt0000000001L5AAI&status=Active	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. No data is saved on the providers servers. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D06 Application Servers	Restricted	Rackspace Servers.	Performance of Contract.	Legitimate Interests, Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Parent Name, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://www.rackspace.com/gdpr Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TNHrAAO&status=Active	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.
D07 Other electronic records including spreadsheets & files	Restricted	Rackspace Servers.	Emails & Cloud Server in the normal business of the organisation.	Legitimate Interests.	Personal Data incl. Student Data, Employee Data, Policies & Procedures.	Authorised Staff Members / Contractors.	Policy: https://www.rackspace.com/gdpr Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TNHrAAO&status=Active	Indefinitely.	N/a	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. Organisational: Relevant employees trained on the Data Protection Policy. Paper records are filed and stored in secure locked cabinets to which only designated employees have access to. Computers on which records are accessible are password protected and are accessible only to designated employees. Office is locked when not in use.
D08 Website	Confidential	Blacknight.	Provide information to the public.	Legitimate Interests.	Personal Data incl. Photos of Academic Achievement Awards, Retirement's etc.	Anyone visiting our website.	N/a	Indefinitely.	N/a	Technical: Individual Logins for Employees. Authentication by using username and password. Access to Server over Encryption / Https / TLS. Organisational: Relevant employees trained on The Data Protection Policy.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D09 Marketing Lists	Restricted	Mailchimp.	Promotion of Business Interest.	Legitimate Interests.	Personal Data incl. Principal Name, School, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	Policy: https://mailchimp.com/legal/privacy/ Privacy Shield Certification: https://www.privacyshield.gov/participant?id=a2zt000000TO6hAAG&status=Active	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Data Protection Addendum in place. Service Provider is Privacy Shield Certified. Recipients of marketing emails have the option of unsubscribing on each email sent. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.
D010 Customer Relationship Database	Restricted	Filemaker Pro Local Database.	Promotion of Business Interest.	Legitimate Interests.	Personal Data incl. Principal Name, School, including phone numbers, email addresses,	Authorised Staff Members / Contractors.	N/a.	Indefinitely.	Hashed Database.	Technical: Individual Logins for authorised staff / contractor members. Access to Local server is restricted to authorised personnel only. Organisational: Relevant employees trained on the Data Protection Policy. Computers on which records are accessible are password protected and are accessible only to designated employees. Offices is locked when not in use.

Data Protection Policy

8.2 Unique School Communications Limited Employee Personnel Files

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D011 Applications, qualifications, references, recruitment, job specification, contract etc.	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D017 Application &/CV										
D018 Qualifications										
D019 References										
D020 Interview: database of applications (the section which relates to the employee only)										
D021 Selection Criteria										
D022 Interview Board Marking Scheme & Boards Notes										

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D023 Job Specification / Description D024 Contract/ Conditions of employment D025 Probation letters/forms D026 Leave of absence applications D027 Job Share D028 Career Break	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D029 Paternity / Maternity Leave	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D030 Force Majeure Leave	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D031 Carer's Leave	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D032 Working Time Act (attendance hours, holidays, breaks)	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D033 Allegations / Complaints	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV, Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D034 Grievance and Disciplinary records	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV, Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

8.3 Occupational Health Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D035 Sickness Absence Records / Certificates	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D036 Pre-Employment Medical Assessment										
D037 Occupational Health Referral										
D038 Correspondence regarding retirement on ill- health grounds										
D039 Accident / Injury at Work Reports	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms, CV Name, Address, Qualifications, Email, Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D040 Medical assessments or referrals	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Health Data.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D041 Sick Leave Records (Sick Benefit Forms)	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Health Data.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

8.4 Superannuation / Pension / Retirement Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D042 Records of previous service (incl. correspondence with previous employers)	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms, CV, Name, Address, Qualifications, Payroll Info.	Authorised members of staff.	N/a	Indefinitely.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D043 Pension Calculation	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms, CV, Name, Address, Qualifications, Payroll Info.	Authorised members of staff.	N/a	Indefinitely.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D044 Salary Claim Forms	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms, CV, Name, Address, Qualifications, Payroll Info.	Authorised members of staff.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years – whichever is the longer.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Data Protection Policy

8.5 Financial Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D045 Accounts	Confidential	Paper: Company Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Point of Contact.	Authorised members of staff. Auditors.	N/a	7 Years.	Confidential Shredding.	Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Organisational: Access to Financial Records is limited to authorised personnel i.e. Managing Director, Auditors, Accounts Personnel.
D046 Payroll and Taxation	Confidential	Paper: Company Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. A Name, Address, Payroll Info.	Authorised members of staff. Auditors.	N/a	7 Years.	Confidential Shredding.	Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Organisational: Access to Financial Records is limited to authorised personnel i.e. Managing Director, Auditors, Accounts Personnel.
D047 Invoices / Back Up Records / Receipts	Confidential	Paper: Company Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Point of Contact.	Authorised members of staff. Auditors.	N/a	7 Years.	Confidential Shredding.	Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection. Organisational: Access to Financial Records is limited to authorised personnel i.e. Managing Director, Auditors, Accounts Personnel.

9 Data Protection Communications

9.1 The Data Protection Policy

This document will be made known to all employees as the primary source of Data Protection Policy at Unique School Communications Limited.

9.2 Privacy Notices

Where information is being collected directly from an individual, a Privacy Notice will be provided at the point at which the data is collected.

- Where information is obtained from another source, a Privacy Notice must be provided:
- If personal data is to be used to communicate with the data subject, at the latest at the time of the first communication with the data subjects;
- If disclosure to another recipient is envisaged, at the latest when personal data is first disclosed.

Privacy Notices will include at a minimum:

- Identification of Unique School Communications Limited as the controller / processor as appropriate of personal data;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subjects' rights as observed by Unique School Communications Limited;

The Privacy Notice will be formatted appropriately for the medium in which it is published. The Privacy Notice is considered an advisory notice regarding Unique School Communications Limited policy and is not intended to constitute a contract with any person.

9.3 Website Privacy Notice

Unique School Communications Limited's main method of informing data subjects and the general public regarding its use of their data whilst on our website will be the Website Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Unique School Communications Limited as the controller / processor as appropriate of personal data;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subject's rights as observed by Unique School Communications Limited;
- Summary technical details regarding information processing (including cookie use); The Privacy Notice will be formatted appropriately for the medium in which it is published.

The Privacy Notice is considered an advisory notice regarding Unique School Communications Limited policy and is not intended to constitute a contract with any person.

9.4 Data Privacy and employees

Employees will be formally notified of Unique School Communications Limited's position with respect to this policy via a briefing.

9.5 Communication plan for Privacy Notices

Unique School Communications Limited will ensure that employees and external parties are informed regarding our use of their data. Any subsequent changes to our policy or practices which affect how user's data is processed will be communicated as per this section.

Employees will be informed directly by email informing of the change, and with attachments or links to supplementary information where required.

Unique School Communications Limited's main vehicle for informing the public of our privacy policy is the Privacy Notice which is published on our website. This will be revised as necessary to ensure compliance.

Where certain classes of users (e.g. schools, parents etc.) need to be informed more proactively regarding our use of their personal data, we will accomplish this by informing them through the app. This will be carried out in advance of the change going live. Where a change of use requires a response, the lack of a response will not be treated as acceptance.

From time to time it will be necessary to revise the Data Protection Policy as well as associated Privacy Notice in response to changes in regulations or evolution of expectations for compliance.

The Privacy Notice itself contains an advisory to users to check regularly for changes.

10 Third parties

10.1 General

Unique School Communications Limited avails of the services of outside parties who act as Data Processors on our behalf to assist us in essential organisation processes. these include but are not limited to IT Systems Development & Maintenance, Data Processing, Finance, Payroll and other Administration.

Unique School Communications Limited will perform due diligence with respect to any and all such third parties and ensure that:

- The basis of the relationship is clearly defined and falls under this Data Protection Policy;
- A Data Processing Agreement / Standard Contractual Clauses are in place that strengthens our compliance with the GDPR;
- Where data held may not come under GDPR, that a non-disclosure agreement protects personal data;

Only providers who are actively involved in processing personal data will come under scrutiny.

10.2 Transfers of personal data to non-EEA jurisdictions

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key organisational processes. Unique School Communications Limited warrants that the use of non-EEA services is an organisational necessity.

In the event we intend to transfer Personal Data to sub-Processor(s) established in a Third Country/ies and if required by the applicable legislation, we shall execute on behalf of the Customer and in its capacity as data exporter, Standard Contractual Clauses. For the avoidance of doubt, all countries other than EU Member States will be considered as Third Countries in the meaning of the GDPR.

Unique School Communications Limited has identified the following Processors and the adequacy arrangements in place to ensure that these transfers are lawful under GDPR:

Processor	Stored in the EU/EEA?	Standard Contractual Clauses
Amazon Web Services	Yes	Yes
Sendgrid	In USA	Yes
Stripe	In USA	Yes
Twilio	In USA	Yes
Unique School App India LLP	Yes	Yes

Amazon

Unique Schools use the services of AWS as our main cloud server provider. Our data and operational systems are stored on these servers. These are all based in Dublin.

Sendgrid (owned by Twilio)

Unique Schools use the services of Sendgrid (a company owned by Twilio) for sending Email messages to App users. This is for email verification on registration and general system emails to app users including reports to school administration staff. The information shared with Sendgrid is Guardians/Parents/Teachers email address, and/or Guardians/Parents/Students name only.

STRIPE

Unique Schools use the services of STRIPE as our Merchant Bank provider for all banking services in relation to our Unique Pay solution. STRIPE are approved by the central bank of Ireland as an authorised merchant bank to operate in Ireland. No student personal data is shared with STRIPE.

Twilio

Unique Schools use the services of Twilio (a US company) for sending SMS messages to App users. This is for OTP on registration and use of SMART texting feature. The information shared with Twilio is Guardians/Parents/Teachers mobile number only. No student personal data is shared with Twilio.

11 Data Security Breaches

Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, Unique School Communications Limited will give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, Unique School Communications Limited will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, our school clients, An Garda Síochána, Insurance company etc.

If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, Unique School Communications Limited may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a sub-processor must be reported to Unique School Communications Limited as soon as the data processor becomes aware of the incident. Conversely, where Unique School Communications Limited is the processor, it too will report the loss of control to the relevant Data Controller.

All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner (DPC) as soon as the organisation becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial / sensitive personal nature. If there is any doubt related to the adequacy of technological risk-mitigation measures then Unique School Communications Limited will report the incident to the DPC.

Unique School Communications Limited will make initial contact with the DPC within 72 Hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be through their website - <https://forms.dataprotection.ie/contact>. The DPC will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

Should the DPC request the company to provide a detailed written report of the incident, it will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data;
- and the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the DPC may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the company has not already done so. If necessary, the DPC may use their enforcement powers to compel appropriate action to protect the interests of data subjects.

Even where there is no notification of the DPC, Unique School Communications Limited will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the company did not consider it necessary to inform the DPC. Such records should be provided to the DPC upon request.

11.1 Data Breach Action Plan

11.1.1 Identification and Initial Assessment of the Incident

- Identify and confirm volumes and types of data affected;
- Establish what personal data is involved in the breach;
- Identify the cause of the breach;
- Estimate the number of data subjects affected;
- Establish how the breach can be contained;

11.1.2 Containment and Recovery

- Establish who (the company, the client etc.) needs to be made aware of the breach;
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause;
- Partial or complete systems lockdown;
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual);

11.1.3 Risk Assessment

- A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish and the risk to data subjects;

11.1.4 Notification

- The school will be notified of all data breaches. They will be provided with all available information and are free, as the data controller, to make their own assessments and decision on risk levels and what reporting is warranted. Unique Schools will supply its findings and recommendations in an urgent and timely fashion.
- On the basis of the evaluation of risks and consequences, the Director in consultation and agreement with the school will decide whether it is necessary to notify relevant stakeholders i.e.
 - the Gardaí;
 - the Data Protection Commissioner;
 - the company's Insurers;
- In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC within 72 hours of the company first becoming aware of the breach.
- If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it affects no more than 100 Data Subjects and it does not include sensitive personal data or personal data of a financial nature, it may not be required to be notified to the DPC. This will be assessed on an individual basis according to the Data Protection Policy on Data Breach above, and where there is any doubt, legal advice will be sought.

11.1.5 Evaluation and Response

- Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Board of Management. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.
- Response may also include updating the Data Protection Policy and retraining employees.

12 Subject Access Requests (SARs)

12.1 Data Subject Rights

Data Subjects are entitled to obtain, based upon a request made in writing to Unique School Communications Limited using the 'Subject Access Request Form' and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The right of the Data subject to:
 - object to Processing of their Personal Data.
 - lodge a complaint with the Data Protection Authority.
 - request rectification or erasure of their Personal Data.
 - request restriction of Processing of their Personal Data.

12.2 Logging Subject Access Requests

All requests received for access to or rectification of Personal Data will be directed to the Director, who will log each request as it is received using the Appendix 6: Subject Access Request Register. The data subject will be asked to fill out the Subject Access Request Form.

12.3 Responding to Subject Access Requests

A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject.

Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Unique School Communications Limited to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If the company cannot respond fully to the request within 30 days, the organisation shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- The name and contact information of Unique School Communications Limited individual who the Data Subject should contact for follow up.

12.4 Protecting Third Parties

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

13 Disposal of Personal Data

Unique School Communications Limited will conduct a regular review of the personal data they hold for the purpose of disposing of redundant personal data. Such a review should take place on an annual basis. Such a review should involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data (see Data Map & Retention Policy in Section 8);

2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Map & Retention Policy in Section 8);
3. Appraisal of the records to determine if they contain personal data which is no longer necessary for the purposes for which it was originally obtained: This step will involve:
 - a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
 - b. Identifying the records for disposal.
 - c. Obtain permission from the Managing Director to dispose of the records.
 - d. Document the disposal of records.
4. Confirmation of disposal to be obtained and documented.
5. Consultation should also take place with the Director for advice on record retention periods and to ensure that records are disposed of in a safe, secure and appropriate manner.

14 Governance Framework

14.1 Supervisory authority

The Irish Data Protection Commission is our lead supervisory authority under GDPR.

14.2 Monitoring Compliance

Unique School Communications Limited will carry out internal GDPR compliance audits against our policy and procedures.

We will also arrange audits of our compliance by independent third parties at longer intervals.

All audit records will remain confidential to Unique School Communications Limited and will be shown only to regulatory authorities on request. Each audit will, as a minimum, assess:

- Compliance with Data Protection Policy in relation to the protection of Personal Data, including:
 - The assignment of responsibilities;
 - Raising awareness;
 - Training of Employees;
- The effectiveness of Data Protection related operational practices, including:
 - Data Subject rights;
 - Personal Data incident management;
 - Personal Data complaints handling;
- The level of understanding of Data Protection Policies and Privacy Notices;
- The currency of Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

14.3 Disciplinary Procedure

Breaches of the GDPR or the company Data Protection Policy may be treated as a matter for discipline and depending on the seriousness of the breach and will be dealt with by the Managing Director in accordance with the company Disciplinary Procedure.

For breaches of the GDPR Regulations, which do not warrant such action, the employee will be advised of the issue and given a reasonable opportunity to put it right.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Blank page



APPENDICES

Appendix 1: Subject Access Request Form

Section 1 – Your details (PLEASE USE BLOCK CAPITALS)

Surname:	
First Name(s):	
Previously known as (if applicable):	
Address:	
Date of birth:	
Telephone number:	
Email address:	

SECTION 2 – Your relationship with Unique School Communications Limited

Are you a current/former* employee?	YES / NO
If yes, please provide the following details: i.e. Month & Year.:	
Are you a current/former client?	YES / NO
If yes, please provide the period which you were a client:	
If neither, please indicate your relationship with Unique School Communications Limited including dates:	

SECTION 3 – PERSONAL DATA REQUESTED

In the box below, please provide as much detail as you can about the personal data you wish to access in order to help us locate it quickly.

In accordance with the GDPR, I request access to the following personal data that I believe Unique School Communications Limited holds about me:
--

SECTION 4 – FEES

No application fees are required for Subject Access Requests
--

SECTION 5 – IDENTIFICATION

In order for us to protect the security of personal data, it is necessary for you to provide proof of your identity. Two forms of identification must accompany this form. Acceptable forms of identification include:

- Copy of passport or driving licence
- ID Card
- Copy of bank statement
- Copy of utility bill

Copies are acceptable in most cases; however, we reserve the right to ask to see original documents where necessary. Copies of such documents sent with your access request form will be securely destroyed once we have verified your identity.

Please complete either section 6 or section 7 as appropriate

SECTION 6 – DECLARATION OF DATA SUBJECT

I confirm that I am the data subject named in Section 1 and I am requesting access to my own personal data. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.

Signed:

Date:

SECTION 7 – DECLARATION OF DATA SUBJECT FOR AGENT TO ACT ON THEIR BEHALF

If you wish someone else to submit a data access on your behalf (e.g. family member, solicitor) please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my subject access request. I have enclosed evidence of my identity referred to in Section 5 and confirm that I want my personal data to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.	
Signed:	Date:

Name of agent:	
Relationship to data subject:	
Address:	
Telephone number:	
Email address:	

RETURNING YOUR COMPLETED FORM:

Please send your completed form (with proof of identity) to: Unique School Communications Limited Unit 38, Block 4, Northwood Court, Santry, Dublin D09 RD63.

FOR COMPANY USE ONLY:

Reference No:	DP/
Date request received:	
Identity verified:	YES/NO
If yes: Original ID supplied in person?	YES/NO
If yes, ID checked and returned to requester? Copy ID attached to request:	YES/NO
If yes, ID verified and documents shredded by:	YES/NO

Privacy Notice for the Data Subject Access Request

The purposes for which Unique School Communications Limited processes your data are:

- To verify your identity;
- To verify your address;
- To establish if you are an adult or a child;
- To identify the personal data for which you have requested a copy;

Legal basis:

- Article 12 of the General Data Protection Regulation;
- In the event that you do not provide the information requested on this form it may not be possible to provide a copy of the data requested;

Categories of data subject:

- Requester of data Categories of personal data;
- Identity including any reference numbers provided;
- Address and other contact details;
- Details of their contacts with the Department where relevant to their request;

Recipients of the data

- The data provided may be shared with the Data Protection Commissioner where requested by that office;

Storage period

- The data processed will be retained for a period of 3 years and subject to review thereafter;

Third Country

- None of your data will be transferred to a country outside of the European Economic Area i.e. the EU and Norway, Iceland and Liechtenstein;

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Contact Details

- Unique School Communications Limited is the data controller for the processing of your data. If you have any query in respect of this you may contact the Director or by post to Unique School Communications Limited, Unit B5, Glasnevin Business Park, Ballyboggan Road, Glasnevin, Dublin 11.

Appendix 2:

Website Privacy Notice

This Privacy Notice governs the manner in which Unique School Communications Limited collects, uses, maintains and discloses information collected from users (each, a “User”) on the website (“Site”). This Privacy Notice applies to the website and our organisation.

Data Controller:

Unique School Communications Limited, Unit 38, Block 4, Northwood Court, Santry, Dublin D09 RD63.
Email: dpo@uniquepublishing.ie

Personal Data (in connection with the provision of services to our school clients):

We use personal data in a variety of ways in connection with the delivery of services to schools. We process this data as per our contractual obligation to the schools we work with.

- **Name and contact data.** We collect your first and last name, email address, mobile phone number, school name, school year, class, P-Pod number and PPS number.
- **Extra-Curricular.** We collect data about the extracurricular activities you (if you are a student) or your child (if you are a parent) participates / is interested in.
- **Contacts and relationships.** We collect data about your child if you are a parent. This data is limited to your child's name, year and class. We collect this data only if the school has certain modules in the App that requires parent/child verification and the data is only used for this purpose.
- **Image.** If you choose to upload your profile photograph to your profile, your image will be stored on our secure server. We request access to the camera on your device in order to do this.
- **Payment data.** If your school app has the School Payment, Bookstore or Uniform Shop we request data necessary to process your payment if you make purchases, such as your Credit Card number and the security code associated with your Credit Card. This data is not stored on our server. We will also collect receipt data or financial transaction data.
- **Device and Usage data.** We collect data about your device and how you and your device interact with the App. For example, we collect:
 - Product use data. We collect data about the items you purchase.
 - Device, connectivity and configuration data. We collect data about your device you use to connect to our App. It includes data about the operating system, operating system version and model and manufacturer. This is to help us to resolve any issues that you may report to use via email using our support email address support@uniqueschools.ie
 - Troubleshooting and Help Data. When you engage Unique Publishing for troubleshooting and help, we collect data about you and your hardware, software and other details related to the incident. Such data includes contact or authentication data, and system and data about App installations and hardware configurations.

How we use collected information (including data processes in connection with the provision of services to our school clients):

We use personal data for purposes including:

- provision and continuous development of our software products;
- provision of customer support;
- provision of training and support to the school;
- to comply with our contractual obligations with the school;
- to promote our legitimate business interests;
- to comply with our legal obligations as limited company;
- to comply with our reporting obligations to various government bodies i.e. CRO, Revenue;
- to provide appropriate training, direction and support to our staff;

How we protect your information:

We adopt appropriate data collection, storage, processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We keep your personal information for a length of time as per our Retention Policy i.e. For our software client's data, this generally means we will retain data for up to 30 days after the contract of service with the school expires. After this time, your data will be disposed of or rendered anonymous. In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in our Data Protection Policy.

Sharing your personal data:

The sharing of personal data and the nature of what is shared depends on various factors. We may also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed. At all times, we shall ensure that the sharing of information is done so as per the requirements of the GDPR.

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key organisational processes. Unique School Communications Limited warrants that the use of non-EEA services is an organisational necessity.

In the event we intend to transfer Personal Data to sub-Processor(s) established in a Third Country/ies and if required by the applicable legislation, we shall execute on behalf of the Customer and in its capacity as data exporter, Standard Contractual Clauses. For the avoidance of doubt, in the case of a No-Deal Brexit (a) the UK will be considered as a Third Country in the meaning of the GDPR for the purpose of this section and (b) all countries other than the UK and the EU Member States will be considered as Third Countries in the meaning of the GDPR.

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent;
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this Statement please contact us below.

Personal Identifiable Information (Website)

We may collect personal identification information from users in a variety of ways in connection with activities, services, features or resources we make available on our Site. We will collect personal identification information from Users only if they voluntarily submit such information to us. Users can always refuse to supply personally identification information, except that it may prevent them from engaging in certain Site related activities.

Non-personal Identifiable Information (Website)

We may collect non-personal identification information about users whenever they interact with our Site. Non- personal identification information may include the browser name, the type of computer and technical information about the users means of connection to our Site, such as the operating system and the Internet service providers utilized and other similar information.

Our use of cookies

Cookies are small pieces of code sent from websites to your device and used to store information by your web browser (see <http://www.youronlinechoices.com/ie/>). Our use of cookies and other technologies may collect information such as your IP address, operating system, the browser you use and the frequency and length of your visits to our website. This information is treated as your personal information by Unique School Communications Limited under the terms of this Statement. We use cookies and other technologies to:

- keep track of how you interact with our website;
- target advertising;
- keep track of how you access and download our materials; and
- offer functionality on our website, including social media plug-ins and sharing.

Changes to this privacy policy

Unique School Communications Limited may from time to time update this privacy policy. We encourage Users to frequently check this page for any changes to stay informed about how we are helping to protect the personal information we collect. You acknowledge and agree that it is your responsibility to review this privacy policy periodically and become aware of modifications.

Links

Some pages of our Website include external links to third party websites. We have no control over and are not responsible for these websites or the use of your information by third parties. You should check the privacy notices on any third party websites to ensure that you are satisfied with their privacy practices, prior to sharing any personal information.

Appendix 3:

App Privacy Notice

This Privacy Notice governs the manner in which Unique School Communications Limited collects, uses, maintains and discloses information collected from users (each, a “User”) on our mobile software applications (“Apps”).

Data Processor (on behalf of the school):

Unique School Communications Limited, Unit 38, Block 4, Northwood Court, Santry, Dublin D09 RD63.
Email: dpo@uniquepublishing.ie

Personal Data (in connection with the provision of services):

We use personal data in a variety of ways in connection with the delivery of services. We process this data as per our contractual obligation to the schools we work with.

- **Name and contact data.** We collect your first and last name, email address, mobile phone number, school name, school year, class, P-Pod number and PPS number.
- **Extra-Curricular.** We collect data about the extracurricular activities you (if you are a student) or your child (if you are a parent) participates / is interested in.
- **Contacts and relationships.** We collect data about your child if you are a parent. This data is limited to your child's name, year and class. We collect this data only if the school has certain modules in the App that requires parent/child verification and the data is only used for this purpose.
- **Image.** If you choose to upload your profile photograph to your profile, your image will be stored on our secure server. We request access to the camera on your device in order to do this.
- **Payment data.** If your school app has the School Payment, Bookstore or Uniform Shop we request data necessary to process your payment if you make purchases, such as your Credit Card number and the security code associated with your Credit Card. This data is not stored on our server. We will also collect receipt data or financial transaction data.
- **Device and Usage data.** We collect data about your device and how you and your device interact with the App. For example, we collect:
 - *Product use data.* We collect data about the items you purchase.
 - *Device, connectivity and configuration data.* We collect data about your device you use to connect to our App. It includes data about the operating system, operating system version and

- model and manufacturer. This is to help us to resolve any issues that you may report to use via email using our support email address support@uniqueschools.ie
- *Troubleshooting and Help Data.* When you engage Unique Publishing for troubleshooting and help, we collect data about you and your hardware, software and other details related to the incident. Such data includes contact or authentication data, and system and data about App installations and hardware configurations.

How we use collected information (including data processes in connection with the provision of services to our school clients):

We use personal data for purposes including:

- provision and continuous development of our software products;
- provision of customer support;
- provision of training and support to your school;
- to comply with our contractual obligations with your school;
- to promote our legitimate business interests;
- to comply with our legal obligations as limited company;
- to comply with our reporting obligations to various government bodies i.e. CRO, Revenue;
- to provide appropriate training, direction and support to our staff;

How we protect your information:

We adopt appropriate data collection, storage, processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We keep your personal information for a length of time as per our Retention Policy i.e. This generally means we will retain data for up to 30 days after the contract of service with the school expires. After this time, your data will be disposed of, or rendered anonymous. In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in our Data Protection Policy.

Sharing your personal data:

The sharing of personal data and the nature of what is shared depends on various factors. We may also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed. At all times, we shall ensure that the sharing of information is done so as per the requirements of the GDPR.

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key organisational processes. Unique School Communications Limited warrants that the use of non-EEA services is an organisational necessity.

In the event we intend to transfer Personal Data to sub-Processor(s) established in a Third Country/ies and if required by the applicable legislation, we shall execute on behalf of the Customer and in its capacity as data exporter, Standard Contractual Clauses. For the avoidance of doubt, in the case of a No-Deal Brexit (a) the UK will be considered as a Third Country in the meaning of the GDPR for the purpose of this section and (b) all countries other than the UK and the EU Member States will be considered as Third Countries in the meaning of the GDPR.

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;

- in some circumstances, request that your personal data be transferred to you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent;
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this Statement please contact us below.

Personal Identifiable Information

We may collect personal identification information from users in a variety of ways in connection with activities, services, features or resources we make available on our app. Users can always refuse to supply personally identification information, except that it may prevent them from engaging in certain app related activities.

Non-personal Identifiable Information

We may collect non-personal identification information about users whenever they interact with our Site. Non-personal identification information may include the device and technical information about the users means of connection to our app, such as the operating system and the Internet service providers utilized and other similar information.

Changes to this privacy policy

Unique School Communications Limited may from time to time update this privacy policy. We encourage Users to frequently check this page for any changes to stay informed about how we are helping to protect the personal information we collect. You acknowledge and agree that it is your responsibility to review this privacy policy periodically and become aware of modifications.

Links

Some pages of our app include external links to third party websites. We have no control over and are not responsible for these websites or the use of your information by third parties. You should check the privacy notices on any third party websites to ensure that you are satisfied with their privacy practices, prior to sharing any personal information.

Appendix 4:

Staff Privacy Notice

Data Controller:

Unique School Communications Limited, Unit 38, Block 4, Northwood Court, Santry, Dublin D09 RD63.

This Privacy Notice governs the manner in which Unique School Communications Limited collects, uses, maintains and discloses information collected throughout the recruitment, hiring and employment of staff.

Personal Data

We collect personal identification information from staff and prospective staff in a variety of ways in connection with your employment at Unique School Communications Limited.

Staff / Recruitment Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payment details;
- Statutory deductions Voluntary deductions;
- Service history;
- Leave including Sick leave / Secondments;
- Qualifications & Results (2nd & 3rd Level) & Work Experience;
- Particulars of your cases where you may query the application of the terms and conditions e.g. Contract of indefinite duration;

How we use collected information

We use your personal data for purposes including:

- your application for employment;
- to provide you with appropriate direction and support in your employment;
- to care for your health and well-being;
- to comply with our legal obligations as an employer;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information

We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We keep your personal information for a length of time as per our Retention Policy i.e. For staff we will retain data for the duration of employment and up to 7 years thereafter. After this time, your data will be destroyed by confidential shredding or deletion from our database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Unique School Communications Limited Data Protection Policy.

Sharing your personal information

From time to time, we may share personal data (arising out of the provision of services or our own company data) with An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc. The sharing of personal data and the nature of what is shared depends on various factors. We may also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed. At all times, we shall ensure that the sharing of information is done so as per the requirements of the GDPR.

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this statement please contact us.

Appendix 5:

Unique School Communications Limited Email Privacy Notice (for inclusion in all email signatures)

Example (in bold below for effect):

Kindest regards,

James Mc Manus F.C.A.
Managing Director

**Unique Publishing, Unit 38, Block 4, Northwood Court, Santry, Dublin D09 RD63, IRELAND.
Tel: 00 353 (0) 1 860 3477 | Mobile: 00 353 (0)87 254 2559**

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

DATA PROTECTION: We're processing data belonging to you i.e. your email address & name as per our legitimate business interests. For more information please review our Privacy Notice here.

Appendix 6: Subject Access Request Register									
REF NO:	NAME OF DATA SUBJECT (PRINT):	DATE INITIAL CONTACT RECEIVED:	RECEIVED BY: (PRINT)	DATE SAR FORM SENT:	DATE SAR FORM RECEIVED:	ID VERIFIED:	DATE SAR PROCESSED:	DATE SAR FULLY RESPONDED TO:	DATE SAR PARTIALLY RESPONDED TO:
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									

Acknowledgement of the Data Protection Policy

I wish to acknowledge receipt of the Data Protection Policy.

Date	Employee Signature	Blocks

US

Data Privacy

Impact

Assessment

Data Privacy Impact Assessment

A DPIA should be completed at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan. Please note that some information provided in the steps below, may also need to be included in Appendix 1. You will need to consult with the third-party service provider for the completion of Appendix 1.

Name of School/College	SCHOOL NAME
Name of proposed Third Party Service Provider	Unique School Communications Limited t/a Unique Schools
Type of New Service	Digital Communications, Administration, Attendance Form management & App Solution

Step 1a: DPIA Screening Checklist		
Does your project involve:	Yes	No
Evaluation or scoring of personal data (including profiling and predicting)		NO
Automated decision-making with legal or similar significant effects		NO
Systematic monitoring including through a publicly accessible place on a large scale		NO
Sensitive data or data of a highly personal nature (including special categories of data and criminal data)	YES	
Data processed on a large scale		No
Matching or combining data sets		No
Data concerning vulnerable people (including children)	Yes	
Innovative use or applying technological or organisational solutions	Yes	
Processing preventing data subjects from exercising a right or using a service or contract		No
If you have answered yes to any of the above questions, you must carry out a DPIA. Please see the DPIA Procedure for further information.		

Step 1b: Identify the Need for a DPIA

Explain broadly what the project aims to achieve and what type of processing of personal data it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA (this can draw on your answers to step 1/ the screening questions).

The Unique Schools Digital Communications, Administration, Attendance forms and App solution creates a single touchpoint for all current parents and students on all school related matters. Only current parents and students have access to the App through a double verification process, so the App platform is private and secure. It centralises all school communications and digitises a large number of paper based processes including Attendance Forms, Notes from Parents, Consent Forms and Payments.

General news and images can be seamlessly shared through API integration with the schools website and social media.

The personal data relating to students includes Name, Year in school, Class, Guardian Name & Mobile number. This data is used identify the students and guardians, to match and verify users during registration and roll over each year. It is used by the school to target communications and assign forms and/payments to the appropriate student/parent/teacher.

Parents can submit information relating to their student through the App to provide the school with information on photograph permissions, medical information, attendance form submission, payments, book ordering (if used).

Step 2: Describe the Processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

how will you collect data?

- Initially data is populated into the Unique Schools System from the schools VS Ware system. This will include Student name, Year, Class, PPOD; Primary contact Name, Mobile number and VS Ware Username; Secondary contact Name, Mobile number and VS Ware Username;
- App users can use the App to submit the following information:
- attendance forms (absentee, late notes, permission to leave early and Return after absence COVID form)
- consent for trips
- Medical Information
- Photo permissions

how will you use data?

Verification - The student data set from VS Ware is used to identify parents/students/teacher during registration. The mobile number is the key mapping data. A OTP is sent to this mobile during registration as a verification procedure.

VS Ware Access - username is prepopulated in VS Ware url which is accessed through the Home menu to assist in easy access to VS Ware for parents

School Information – All other forms and data submitted by parents is used by the school for general day to day school administration – Attendance, Permissions etc

how will you store and delete data?

Storage – All Data is stored on our cloud based servers within the EU

Delete – All Data is retained in line with the schools directions and their legal obligations on data retention. Data is deleted after expiration of the appropriate period and in line with GDPR requirements where a user requested to be deleted.

What is the source of the data?

- 1) The Student Data set comes from your VS Ware Attendance System and this is updated annually.
- 2) Other data is submitted by App users through the App

Will you be sharing data with anyone?

NO. The data supplied and collected through the App is the schools data and we only process the data in line with our DPA with the school. The information is never shared with any third party.

What types of processing identified as likely high risk are involved?

We do not describe any of our process as high risk.

Describe the scope of the processing:

What is the nature of the data:

The data is student/parent information required by the school to carry out its day to day administration and communication obligations. Specific data as listed above.

Does it include special category:

Data will relate to children between the ages of 12 and 17.

or criminal offence data?

No data on criminal offences is collected or held.

How much data will you be collecting and using?

This will vary on a student by student basis. The data being collected is required by the school to carry out administration of the school and all data collected is necessary for this.

Student Data will include:

- Student name, Year, Class, PPOD; Primary contact Name, Mobile number and VS Ware Username; Secondary contact Name, Mobile number and VS Ware Username;
-

App users can use the App to submit the following information:

- attendance forms (absentee, late notes, permission to leave early and Return after absence COVID form)
- consent for trips
- Medical Information
- Photo permissions

How often?

Data such as attendance information is submitted by parents daily. Various forms can be submitted a few times a year

How long will you keep it?

All Data is retained in line with the schools directions and their legal obligations on data retention. Data is deleted after expiration of the appropriate period and in line with GDPR requirements where a user requested to be deleted.

How many individuals are affected?

All students and parents and teachers attending the school.

What geographical area does it cover?

The local geographical area in which the school is.

Describe the context of the processing:

what is the nature of your relationship with the individuals?

All App users are parents/students/teachers attending or working in the school.

How much control will they have?

They have full control. They can decide not to download the App. For those who do download

Would they expect you to use their data in this way?

YES – all data is used specifically in line with the suers permission and expectation.

Do they include children or other vulnerable groups?

Yes - Data will relate to children between the ages of 12 and 17.

Are there prior concerns over this type of processing or security flaws?

No. Unique Schools are currently working with over 140 schools in Ireland and there have been no security issues since its launch in 2015.

Is it novel in any way?

Yes. It pulls everything into one single platform. This centralises communications and administration and allows for the digitisation of many paper based processes.

What is the current state of technology in this area?

Apps and digital communications have been standard in many industries and areas for many years.

Are there any current issues of public concern that you should factor in?

NO.

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

No

Describe the purposes of the processing:

what do you want to achieve?

Centralise all communications and administration processing and access into one single platform. Remove duplication of work. Integrate publishing across all channels. Digitise paper processes. Improve engagement with parents and students. Reduce costs on SMS and postage.

What is the intended effect on individuals?

Make access to school information more centralised and the submission of data and forms more seamless and transparent.

What are the benefits of the processing for you, and more broadly?

Centralise all communications and administration processing and access into one single platform. Remove duplication of work. Integrate publishing across all channels. Digitise paper processes. Improve engagement with parents and students. Reduce costs on SMS and postage.

Step 3: Consultation process

Consider how to consult with relevant stakeholders:

describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

A full presentation of the system will be given to all senior management of the school by the Managing Director of Unique Schools. The relevant documents will be gathered and reviewed by the relevant IT and GDPR appointed personnel in the school and at ETB level as part of the review process.

Who else do you need to involve within your organisation

All appropriate staff will be involved.

Do you need to ask your processors to assist?

Unique Schools will liaise with appropriate staff in the school and ETB to answer all questions and provide necessary information to assist in a full assessment of the solution and the companies adherence to GDPR, security and best practice.

Do you plan to consult information security experts, or any other experts?

Unique Schools has provided details regarding the levels and methodologies of security which they have in place. All data is stored with AWS who have a very high level of data security in place.

Step 4: Assessment of Necessity and Proportionality of Processing

Describe compliance and proportionality measures, in particular:

what is your lawful basis for processing?

All information sought, submitted and processed is required by the school in line with legal obligations, administration practicalities and best practice to meet the educational needs of the student.

Does the processing actually achieve your purpose?

YES.

Is there another way to achieve the same outcome?

Currently we are achieving a less than optimum outcome through the use of a fragmented, un integrated, variety of platforms and paper based processes.

How will you prevent function creep?

The system is highly automated and information submitted is directed toward the intended purpose only. Access to data and reports are assigned on a “need to know” basis.

How will you ensure data quality and data minimisation?

Data is submitted by the end user (parent) or prepared by the School. There is a double verification process during registration which gives certainty over registered users. Many forms have mandatory fields which ensure full and complete data is submitted and only necessary data is sought and collected.

What information will you give individuals?

All users can access information on the App prior to downloading. They are also asked to read and accept all terms and conditions before completing the registration process.

How will you help to support their rights?

Unique Schools is the leading provider of Digital Communications & Administration systems for schools in Ireland and a highly respected and professional company. They provide a full Policies and Procedures document which details all their processes and procedures on GDPR matters. Their staff are available by email and telephone support and queries for all app users and school staff.

What measures do you take to ensure processors comply?

A Data Processing Agreement is completed in advance of the commencement of any work.

How do you safeguard any international transfers?

Unique Schools specifically state that all data is held in line with their GDPR obligations in their documentation.

STEPS 5 & 6: RISK ASSESSMENT - IDENTIFYING PRIVACY RISKS AND EVALUATING PRIVACY SOLUTIONS						
Risk Register Owner:					Assessment of Risk (Low / Medium / High)	
No.	Description of Risk and Hazard	Consequence	Current internal CONTROLS (Provide details of how you currently manage the risk)	L	M	H
1	Unauthorised School staff access to CMS	Unauthorised user can access data	Double verification process during registration for all staff via email and mobile. Mobile number matched to schools data. Unique log in for each user System access to granted based on permissions	Low		Verification at registration is mandatory School senior staff controls mobile numbers provided Access permissions can only be provided by Unique Schools Team at Super Admin Level Unique Schools are risk owner
2	Cyber Attack	Potential Loss of control of Data Potential Loss of access to data/systems	All Data is on AWS servers Firewalls in place Back up procedures Regular monitoring and updating of cyber security procedures	Low		Use of third party servers who provide highest level of security Unique staff are given regular updated training Quarterly review of procedures and new technologies available and changes in systems/processes

Step 7: Document DPIA Outcomes		
Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Residual risks approved by:		If accepting any residual high risk, consult the Data Commissioner before going ahead
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 1
GDPR Requirements

To be completed by the school and the Unique Schools

	School Name	Unique Schools
What data is collected?		Student name, year, class, DOB, PPOD, parents name, parents mobile number, parents email, medical information, attendance data, consent forms,
Why is the data collected?		To enable communications with school, parents and students and process forms and other information in line with operation of the Unique Schools system
How is the data collected?		Parents submit data via the schools App
What format is the data stored in?		All data is encrypted at rest and in transit
What security measures are in place to ensure that the data remains secure and confidential?		We use AWS as a leading provider of cloud based server solutions and best in class security All data is encrypted at rest and in transit Verification processes in place to gain access to system Parents can implement PIN security Teachers have PIN security on Comms App Access to information is granted on need to know only All US staff are trained on importance and implementation of security Unique School have engaged Ansec Ltd a cyber security specialist to

		review and ensure all areas are best in class and to assist with achieving ISO 27001
Where is the data hosted?		AWS Servers in Dublin
Who has access to the data? What processes are in place to ensure against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data?		We use AWS as a leading provider of cloud based server solutions and best in class security All data is encrypted at rest and in transit Verification processes in place to gain access to system Parents can implement PIN security Teachers have PIN security on Comms App Access to information is granted on need to know only All US staff are trained on importance and implementation of security Unique School have engaged Ansec Ltd a cyber security specialist to review and ensure all areas are best in class and to assist with achieving ISO 27001
Do we share the data with third parties? If so, who and why?		Twillo & Sendgrid provision of SMS & Email services
If the data is mandatory and is not provided, what are the repercussions for the individual?		Student Data set (student name, class, year, DOB, PPOD, Parents name & Mobile) are required to run the system and validate users. Without this data parents/students cannot get access to the App
If the data is discretionary and is not provided, what are the repercussions for the individual?		<i>If parent/students do not provide information required through the App (Attendance forms, Consent forms etc) then they will have to provide data in hard copy to the school for processing</i>
What is your records retention policy in regard to data held for this purpose?		<i>Data is retained in line with schools legal obligations</i>

Please confirm that the data will not be used for any marketing purposes.		<i>There is no marketing processing of data</i>
Please confirm that personal data shall not be transferred to a country or territory outside of the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.		<i>Unique Schools confirm</i>
Completed by:		<i>James McManus Managing Director</i>
Reviewed by:		

US

Group

Business

Structure

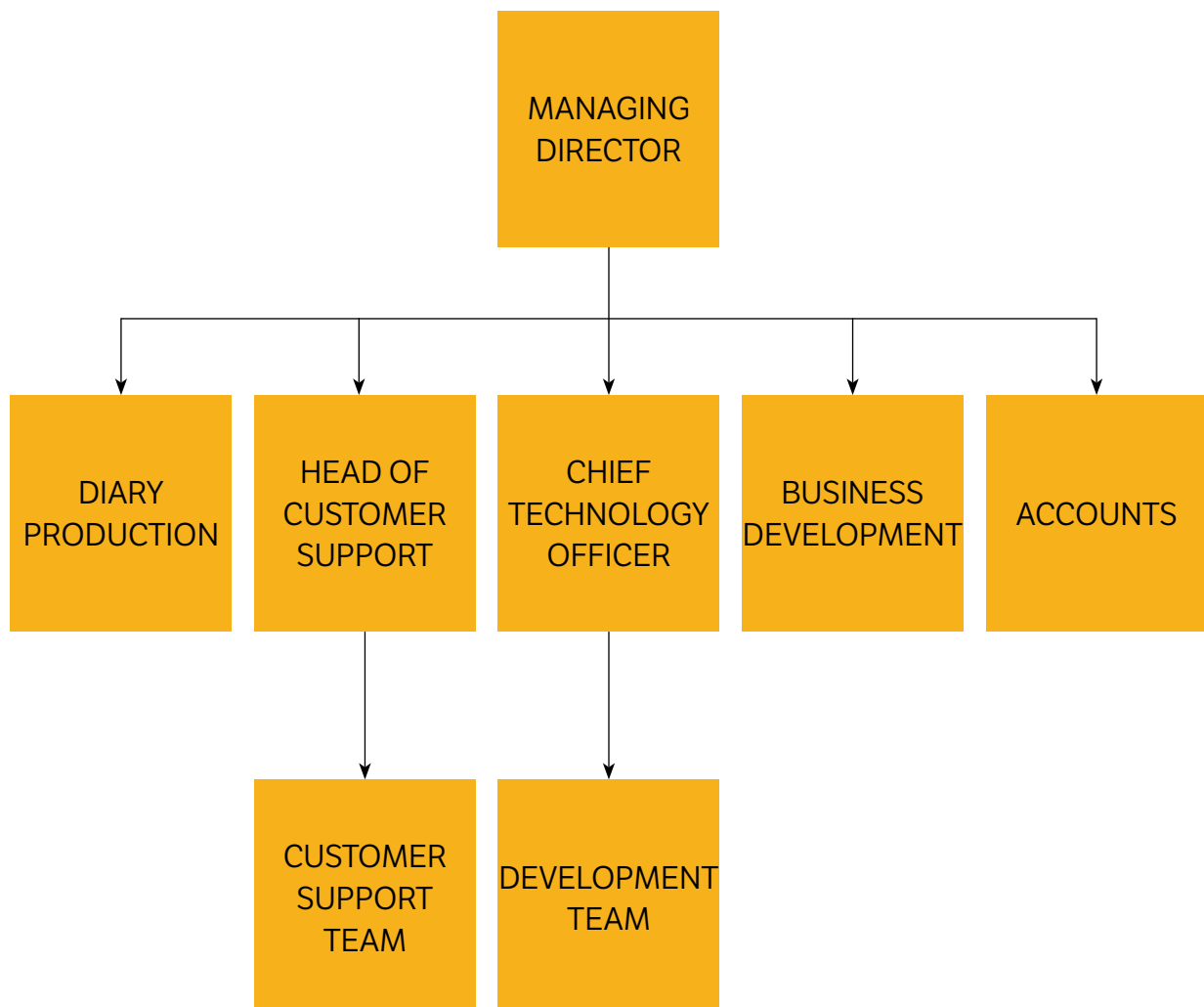
UNIQUE SCHOOL COMMUNICATIONS LTD
T/A UNIQUE SCHOOLS

OWNERSHIP: James Mc Manus 100%

LOCATION: Dublin

STAFF: 9

Main operating business for Unique Schools digital communications, administration, attendance form management, app systems and student diary design and production.



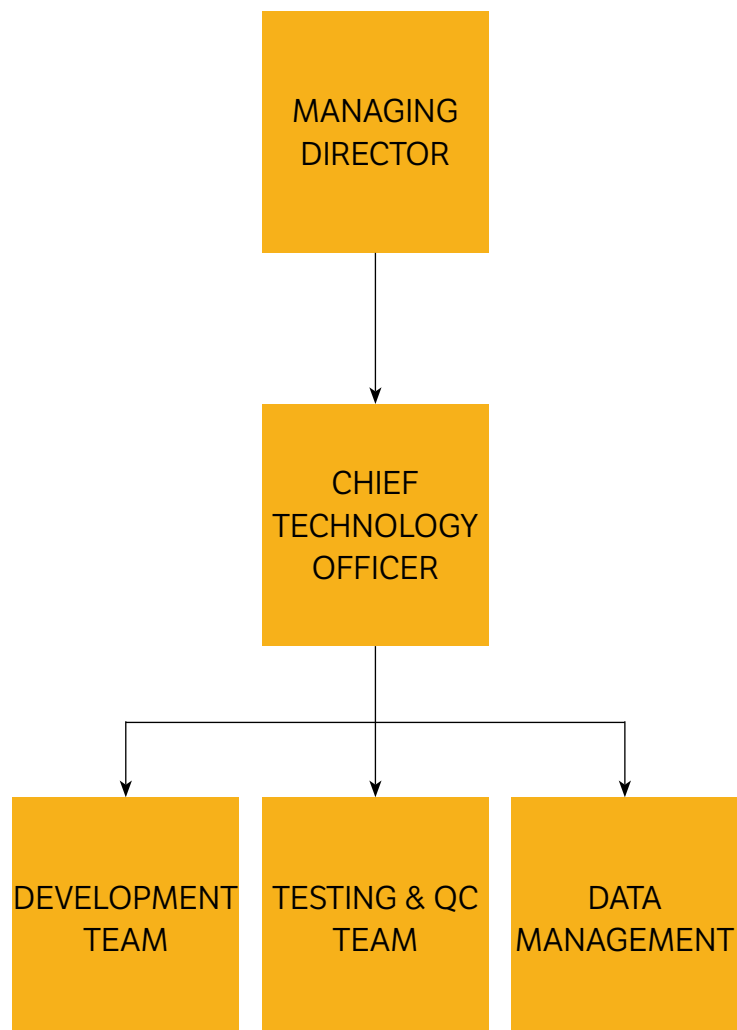
UNIQUE SCHOOL LLP INDIA

OWNERSHIP: James Mc Manus 80%
Ravindra Cherke 20%

LOCATION: Mumbai

STAFF: 14

Main IT development, management and services business supporting Unique School Communications Ltd, Dublin. This company is 80% owned and fully controlled by James Mc Manus as a subsidiary support business. Unique School Communications Ltd is the sole customer of Unique School App LLP.



UniqueSchools

**Address**

Unit 38, Block 4
Northwood Court
Santry
Dublin 9
D09 RD63

Mobile

James McManus (Managing Director)
087 254 2559

Email

james@uniqueschools.ie

Web

www.uniqueschools.ie