Data Protection Policy

Effective Date: 01-09-2011

Document Owner:	Lawford Education Ltd

Version

Version	Date	Description	Author
1.0	01-09-2011	Data Protection Policy created	Tim Ballard
1.1	06-01-2014	Updated with further information on data security	Tim Ballard
1.2	01-09-2017	Updated with further information on data security	Tim Ballard
1.3	01-04-2018	Updated to comply with GDPR	Tim Ballard

Approval

Approvers	Role	Signed	Approval Date
Lawford Education Ltd	Service Provider		01-09-2011, 06-01-2014, 01-09-2017, 01-04-2018

Data Protection Policy

This policy sets out how Lawford Education Ltd uses and protects any information that is provided to them by educational organisations such as schools. 'We', 'us' or 'our' in this document refers to Lawford Education Ltd. 'You' or 'Your' refers to an organisation that uses our services.

This policy may change from time to time but we will inform all organisations that are affected and give appropriate notice before implementing changes. This policy is effective from 1st September 2011.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. We are committed to ensuring that we adhere to the data protection principles which are set out in the General Data Protection Regulation (2016). Data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Tim Ballard, as Managing Director, is the designated data controller for Lawford Education Ltd. Any employee or client should direct any data protection matters to his attention as soon as possible so that appropriate action can be taken.

What we collect

For the most part, we only collect data that is necessary for running the system, which is in accordance with the GDPR (2016). We may collect the following information.

Data	Required?	Why we need it
Student name (surname, forename)	Yes	Used for the management of student accounts and associating points data with each student
UPN (unique pupil number)	No	In order to update class lists and keep student details accurate on Pupil Reward Points, we once used the UPN to identify students (especially when there were two students with the same name). However, our system now uses admission number as it is less sensitive than a UPN.
Admission number	Yes	We use this a unique identifier.
Year group, registration group, house group, class lists	Yes	This allows the system to produce leaderboards and it allows staff to easily award points to students in these groupings
Attendance data	No	We need this if you would like to show a student their attendance, or award points automatically based on attendance
Punctuality data	No	We need this if you would like to show a student their punctuality, or award points automatically based on punctuality
Pupil Photos	No	We can extract pupil photos from SIMS so that pupil photos can be displayed to staff users when awarding points.
Gender, Free School Meal Eligibility, Pupil Premium flag, English as Additional Language flag, SEN status	No	Providing this information will allow staff to run reports that show how many points each of these subgroups is receiving.
Total behaviour points	No	If you use SIMS to record behaviour, we can import this daily to display to students or staff
Staff name (title, forename, surname), teaching position	Yes	Used for the management of staff accounts and associating points data with each member of staff. Teaching position can also be used for access control.
Student email addresses	No	This is required if you would like students to be able to retrieve their password using the “forgot my password” feature

Data	Required?	Why we need it
Staff email addresses	No	This is required if you would like students to be able to retrieve their password using the "forgot my password" feature. In addition, staff can be sent automatic email notifications when particular events occur such as when rewards are claimed.
Parent data (parent name, email, relationship, child UPN)	No	If you would like to provide separate user accounts for parents, we need basic details to allow them access to only their child's data.
Other data	No	You are welcome to send us additional data for the purpose of displaying it to staff or students. This data will not be used for any other purpose unless requested.

What we do with the information we gather

You remain the owner of your data and you can request it at any time. We require your data in order to provide you with a good service and to understand your needs. In particular, we use your data for:

- Operating the system for which you have paid your subscription.

- Internal record keeping.

- We may use the information to improve our products and services.

- We may periodically send promotional emails about new products, special offers or other information which we think you may find interesting using the Administrator email address which you have provided.

- From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your interests.

Removing a school's data

In line with our data protection obligations, we only store data for as long as necessary. Therefore, when a school terminates their service, or requests that their school's data is removed, the following process is started. Schools must make the request in writing (an email is sufficient).

Within 48 hours	A confirmation email will be sent to the school administrators.
48 hours later (or before)	The data will be removed from the online system.
30 days later	The final backups that contain the data that was removed from the online system are deleted. Before this time, we will also ensure that any offline data is removed.*
After this time	The data cannot be recovered.

*Please note that we may retain some email communication for longer than 30 days to provide an audit trail such as the email request to delete the data.

Data Security

We are committed to ensuring that your data is secure. To prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure data. All data is stored on servers based in London, UK.

Network

- Always high-performance bandwidth
- Nine network providers, for multiple redundancies
- Fibre carriers enter at disparate points to guard against failure
- Network topology and configuration automatically improves in real time
- We use fully managed Rackspace Hosting. The same is used by:
    - Royal Navy
    - NHS
    - Department for Transport
    - Vodafone etc.

Precision environment

- The data centre's HVAC (Heating Ventilation Air Conditioning) system is N+1 redundant. This ensures that a duplicate system immediately comes online should there be an HVAC system failure.
- Every 90 seconds, all the air in the data centre is circulated and filtered to remove dust and contaminants.
- The advanced fire suppression system is designed to stop fires from spreading in the unlikely event one should occur.

Core routing equipment

- Only fully redundant, enterprise-class routing equipment is used.
- Fibre carriers enter the data centre at disparate points to guard against service failure.

Physical security

- Keycard protocols, biometric scanning protocols and round-the-clock interior and exterior surveillance monitor access to the data centre. Manned by security team 24/7/365.
- Only authorised data centre personnel are granted access credentials to the data centre. No one else can enter the production area of the data centre without prior clearance and an appropriate escort.
- Every data centre employee undergoes multiple and thorough background security checks before they are hired.
- Access to data halls themselves and other secure subareas is forbidden. Visitors must sign the visitor's log, present a valid photo ID, and specify the reason for visiting and a point of contact. Visitors are escorted at all times.

Conditioned power

- Should a total utility power outage ever occur, the data centre's power systems are designed to run uninterrupted, with every server receiving conditioned UPS (Uninterruptible Power Supply) power.
- The UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails.
- If an extended utility power outage occurs, the routinely tested, on-site diesel generators can run indefinitely.

Network technicians

- Networking and security teams working in the data centre are required to be certified. They must also be thoroughly experienced in managing and monitoring enterprise-level networks.
- The Certified Network Technicians are trained to the highest industry standards.

Personnel

- Our staff are required to sign a confidentially / non-disclosure agreement.
- Our staff must adhere to the company's password management policy.

Segregation of data and storage

- Organizations' data is logically separated - different location of encrypted data on the hard disk as well as different database / tables.

- Data received from Management Information Systems is processed immediately or stored in a non-publicly accessible location then processed within 24 hours. Once processed, the data is stored in password-protected database tables, which are not publicly accessible. Data extraction from API's is done via a secure connection.

For more information on how we secure data, please use the contact form on our website.

We advise all our users to set strong passwords and provide tools to assist with choosing a password of an adequate strength. However, ultimately, we cannot be held responsible for unauthorized access to our systems caused by your negligence. This includes but is not limited to sharing usernames and passwords, allowing staff or students to set weak passwords, not changing the default password assigned to students or staff.

We backup your data on a daily basis to ensure its safety. This allows us to restore the data, if it becomes corrupted, is deleted or is modified without authorization.

You are responsible for users (including staff, students) complying with your organization's own data protection policy and GDPR when using data that is taken from our website, especially data of a sensitive nature.

Serious Incident Plan (in event of data loss or breach)

Containment and recovery – where a data breach has been identified by Lawford Education Ltd, the designated data processor will investigate and use all appropriate resources to contain the situation by preventing further loss of data and / or recover lost data. If deemed necessary, the data processor will inform the police of the incident.

The data processor will assess the risks of the data loss, which will be determined by whether it involved a criminal act such as theft of data or unauthorized access, whether the data included sensitive data, the number of people affected, the type of people affected (staff, students, parents etc.), and the potential consequences for individuals.

Notification of breaches – the data processor will notify the system's lead administrator at the school where the breach has taken place. We will use the school telephone number in the first instance and then send an email if the administrator is unreachable. Where possible the email will contain details on what occurred, when it occurred, the status of containment, what data was revealed and to whom, and any recommended actions to mitigate risks associated with the breach.

If the breach included personal data, the data processor will inform the ICO.

Evaluation and response – where there has been a serious incident, we will review all associated procedures and security measures to minimize the likelihood of similar incidents occurring in the future.

This plan has been formed via a review of the guidance of data security breach management provided by the ICO.
https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this data protection policy. You should exercise caution and look at the privacy statement applicable to the website in question.

Processing your personal information

You may choose to restrict the collection or use of your personal information in the following ways:

- If you would not like us to send promotional emails to the Administrator email address, you may let us know at any time by writing to or emailing us at support@pupilrewardpoints.co.uk.

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so.

Any user may request details of personal information which we hold about them under the Freedom of Information Act. A small administration fee will be payable, which we may choose to waive. If you would like a copy of the information held for your organization please write to Mr Ballard, Lawford Education Ltd, 11 Waldegrave Way, Lawford, Manningtree, Essex, CO11 2DX. We will comply with such requests as soon as possible but no later than 40 days as required by the 1998 Act.

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible at the above address. We will promptly correct any information found to be incorrect.

Data subject access requests

We will respond to any request for an individual's personal data by that individual, or organisation's data by that organisation. We will respond within 30 days and can provide information regarding what personal data is being processed, the reasons for it being processed and who has access to the information. We can provide a copy of the data, which may be subject to a fee.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Designated Data Controller.