De La Salle College

Compiled by: Mr S Barrett	Date: May 2018
Policy Holder: Mr S Barrett	Revision date: July 2018

OUR DATA CONTROLLER (DC) IS JASON TURNER (HEADMASTER)

OUR DATA PROTECTION OFFICER (DPO) IS SIMON BARRETT (ASSISTANT HEAD)

As a private school, De La Salle College is a data controller and holds data on its students in order to support their teaching and learning, to monitor and report on their progress, to provide appropriate pastoral care, and to assess the school's performance. This data includes contact details, Examination and assessment results, attendance, special educational needs and any relevant medical information. The data we hold must only be used for specific purposes allowed by law. This statement outlines the types of data held, why that data is held, and to whom it may be passed. For the purposes of the Data Protection Law (Jersey) 2018, De La Salle College is deemed as a "public authority" being "any other body (whether incorporated or unincorporated) that exercises functions of a public nature. The data controller is registered under Article 17 of the Authority Law (Jersey) 2018.

De La Salle College holds personal data concerning its' student body, the parents'/guardians' of said students and its' alumni. De La Salle College processes this data on the basis of schedule 2 (Article 9) of the Data Protection (Jersey) Law of 2018, (specifically to fulfil the Public functions (paragraph 4) detailed in the Education (Jersey) Law of 1999) for the purposes of legitimate interests (paragraph 5), to fulfil other legal obligations (paragraph 7) and Article 29. De La Salle College holds personal data concerning its' employees and former employees. De La Salle College processes this data on the basis of schedule 2 of the Data Protection
(Jersey) Law of 2018 specifically, to fulfil its' obligations regarding Employment and Social fields (paragraph 8). De La Salle College holds personal data concerning its' student body, the parents'/guardians' of said students, its' alumni, its' employees and former employees. De La Salle College processes this data on the basis of schedule 2 of the Data Protection (Jersey) Law of 2018, specifically to fulfil the Vital Interests of the data subject or another person (paragraph 9) in order to fulfil its statutory safeguarding responsibilities. Finally De La Salle College holds and processes data on students, parents, alumni, employees and former employees, processing this data by virtue of schedule 2 of the Data Processing (Jersey) Law of 2018, specifically where the data subject has given specific consent. Data will be retained by the College for periods as prescribed in the destruction of data schedule that forms part of this policy. Resources to enable this schedule to be completed are made available by the Data Controller. The implementation of this schedule is policed by the Data Protection Officer and is subject to annual external verification.

The data we hold, including emails and web data, is stored on servers hosted on site. Where this is not possible due to a particular software issue or because the data needs to be processed by a third party, for example examination data, this is subject to a service level agreement that clearly stipulates the use of the data, its' security and the length of time the data may be held by the third party processor before it is to be destroyed. These service level agreements are reviewed by the DPO to ensure that they comply with part 8 of the Data Protection Law (Jersey) 2018 and the GDPR which govern Cross-border data transfers, prior to signature from the DC. Where data is the subject of a Cross-border data transfer but is not covered by

All service level agreements relating to a third party data processor it will be recorded by the College and this log is subject to examination by the Office of the Data Commissioner.
Our websites do not automatically capture or store personal information, other than logging the user's IP address and session information such as the duration of the visit and the type of browser used. This is recognized by the web server and is only used for system administration and to provide statistics. Should you wish to contact us, you will be asked to submit some personal information (e.g. your name and email address). By entering your details in the fields requested, you enable us to provide you with information you require. Your message and details may be passed on to colleagues who are better able to answer your questions.

For safeguarding purposes all emails written and or dispatched, any website searches undertaken or webpages visited are screened to comply with our legal obligations. De La Salle College processes this data on the basis of schedule 2 of the Data Protection (Jersey) Law of 2018, specifically to fulfil the Public functions (paragraph 4) detailed in the Education (Jersey) Law of 1999, for the purposes of legitimate interests (paragraph 5), to fulfil other legal obligations (paragraph 7) and Employment and Social fields (paragraph 8). All users of computers at De La Salle College are reminded of their obligations to act in accordance with our Safeguarding policy (and other relevant Safeguarding and Professional standards) when they log on to a computer and students are made aware of this via E-safety lessons. The screening software is hosted by servers on site.

De La Salle College uses CCTV to monitor its premises and adjacent areas in order to maintain security and to prevent and investigate crime. This data is held for a period of 30 days on servers hosted at the College and is then destroyed. This data can only be viewed by employees of the College for safeguarding, pastoral and behaviour purposes with the express written permission of the Data Controller. A record of each view data is retained by the College SIRO and by the College Data Protection Officer. We may on occasion share this data with a third party, for example the police force. Where this data release is requested it will be done on the legal basis of paragraphs 4 or 19 of schedule 2 of the Data Protection Jersey Law (2018). The release of data will be reviewed by the DPO and can only be sanctioned by the DC.

De La Salle College uses photographic images in its publications and on its websites, under paragraph 5 of schedule 2 of the Data Protection Jersey Law (2018). We will not publish photographs of individuals alongside their names without the express consent of the data subject or the individual with Parental Responsibility for the data subject.

As part of our admissions procedure we collect details of candidates and their parents or guardians and information regarding their education history. This information may be used for administrative or legal purposes during the admissions process. (Paragraphs 4, 5 & 7 of schedule 2 of the Data Protection Jersey Law 2018). Should the application be unsuccessful this information will be securely destroyed as per the destruction schedule.

When a pupil accepts a place at De La Salle College further data may be collected in addition to that submitted as part of the admissions process. This might include: medical records and information, including details of any illnesses, allergies or other medical conditions suffered by pupils; personal details such as home address, date of birth and next of kin; information concerning pupil’s performance at school, including their discipline record, School reports and examination results; financial information including information about the payment of fees; biometric data – specifically finger pattern technology. This information is kept

electronically on the College's information management system and/or manually in indexed filing systems. (Paragraphs 4, 5, 7 & 9 of schedule 2 of the Data Protection Jersey Law 2018). Except as might be required by law (see below), we do not share data with external bodies or third parties unless the data subject or the person with parental responsibility has given their written consent or one of the specific exemptions under the Data Protection Law applies (please refer to the Data Protection (Jersey) Law 2018). In the event of any request from a third party to share data it will be subject to a review procedure undertaken by the Data Protection Officer (DPO), who will establish the legal justification for the release of the data, the manner in which the data is transferred to ensure security, the purpose for which the data is to be used and finally the amount of time the third party may hold the data before it is to be destroyed or returned to the College. Where De La Salle College receives a data release request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. If the data requested can be pseudonymised the College will release the information in this form. Once this process has been undertaken data will be released only with the specific authority of the Data Controller (DC). All data transfers to a third party will be recorded by the College and this log is subject to examination by the Office of the Data Commissioner.

From time to time, the College is required to pass on data to the Department for Education, in accordance with paragraph 4 of schedule 2 of the Data Protection Jersey Law 2018. When a student has transferred to another educational establishment, upon request we will pass on all information relevant to the education and care of that pupil, in accordance with paragraph 4 of schedule 2 of the Data Protection Jersey Law 2018. This transfer is the main way in which the Data subjects right to data portability is exercised and this method is agreed with the Department for Education. We will inform the person with parental responsibility for the data subject when we have transferred the data to the new educational establishment. Again in accordance with paragraph 4 of schedule 2 of the Data Protection Jersey Law 2018, data may also be passed directly to UK examination and assessment organisations for processing. The resultant information is returned to De La Salle College and in the case of public examinations also to the Department for Education, to enable Island wide statistical analysis. Contact details are provided to the Department for Health and Social Services and Family Nursing & Homecare in order that parents may be contacted regarding child health programmes, such as the dental screening scheme and the vaccination programme, in accordance with paragraph 16 of schedule 2 of the Data Protection Jersey Law 2018

Data supplied to the Department for Education about students from De La Salle is only used to carry out its Public functions, that is: to evaluate and develop education policy and to monitor the performance of the education service as a whole. Information will also be used to assess any special educational needs the pupil may have. The Department for Education also uses the information to derive statistics to inform decision-making on (for example) the funding of schools, and to assess the performance of schools and set targets for them. Information may be shared by the Department for Education with other States Departments or agencies for statistical or research purposes, or with Social Services or other relevant agencies for the purposes of safeguarding. Information is also passed to the Population Office and the Statistics Unit in accordance with the States of Jersey's public function and legal obligations.

The Data subject or those with Parental Responsibility have the right to object to processing of any personal data based exclusively on the conditions of public functions or legitimate interests. If the Data subject or those with Parental Responsibility wish to exercise this right

they should inform the DC in writing. However, this cessation of data processing does not apply where the DC demonstrates that there are compelling legitimate or public interests in continuing to process the data that outweigh the interests' rights or freedoms of the data subject.

PROCEDURE FOR RELEASE OF DATA

All requests to release data either as part of data access request or to a third party will go through a review process conducted by the DPO.

Category A: Data request to a third party such as the Education department or the Department for Health which are already governed by a Service Level Agreement. Where there is an existing data processing agreement in place which relates to processing under specific schedule 2 processing as outlined in the Data Protection (Jersey) Law of 2018, the risks to data are relatively small as the transfer is being made to a public authority, registered with the Data Protection Authority and operating according to similar principles to DLS College. Requests for Category A data release should be sent to the DPO for checking. The DPO will then forward the request to the DC for approval and permission to release the data. Data should only be released using the agreed methods of data transfer, that is secure encrypted USB drive which is signed for by an officer of the SOJ . The data should only be transferred with a clear statement outlining the purpose for which the data is to be used and an assurance that the data will be held securely, not passed to other third parties and destroyed when no longer needed.

Category B: Data transferred to a third party for data processing where the data will be stored in the UK or in the EU which is already governed by a Data Processing Agreement. Where there is an existing data processing agreement in place as outlined in the Data Protection (Jersey) Law of 2018, the risks to data are relatively small as the transfer is being made to a UK based organisation such as an examination board which commits to following the precepts of the European Union's General Data Protection Regulation (GDPR). Where the Data transferred is to a third party for data processing where the data will be stored in the UK or in the EU but which is not yet governed by a Data Processing Agreement. The DPO will need to establish a DPA with the third party and be satisfied that the principles within the GDPR will be completely complied with. This will inevitably take longer but no data can be transferred without said DPA being in place.
Requests for Category B data release should be sent to the DPO for checking. The DPO will then forward the request to the DC for approval and permission to release the data. Data should only be released using a means approved by the DPO. The data should only be transferred with a clear statement outlining the purpose for which the data is to be used and an assurance that the data will be held securely, not passed to other third parties and destroyed when no longer needed.

Category C: All other data transfer requests. Requests for data transfers that do not fall within Category A or B will normally only be considered providing the data can be pseudonymised or explicit consent has been gained from the Data subject or the person acting with parental responsibility for the data subject.

Requests for Category C data release should be sent to the DPO for checking. All category C requests will need to go through a data protection impact assessment for high risk processing conducted by the DPO. The DPO and DC will then consider the impact assessment before either refusing or granting permission to release the data. Data should only be released using a means approved by the DPO. The data should only be transferred with a clear statement outlining the purpose for which the data is to be used and an assurance that the data will be held securely, not passed to other third parties and destroyed when no longer needed.

Data Release Form

Please complete this form at the earliest opportunity, and before entering into any contracts. Ensure it is signed by the Data Protection Officer and submitted to the Data Controller.

Do not alter the format of this document in any way.

Third Party requesting data	
DLS staff processing request	
Proposed Data Release (be specific) Category A/ B / C (delete as appropriate)	
What is the justification for the Data release?	
What is the legal basis for the Data Release?	
How is the data to be transferred?	

How long will the data be retained by the Third Party?	

Agreement to release Data

DPO Name	Signed	Date
DC Name	Signed	Date

A copy of this completed form will be sent to you. See overleaf for conditions/action plan set by the DPO. This form will be retained by the DPO for six years following the DATA request.

Pupils, parents, staff and alumni, as data subjects, have certain rights under the Data Protection Law (Jersey) 2018, including a general right of access to personal data held on them, with those who have parental responsibility exercising this right on their behalf if they are too young to do so themselves. If you wish to access the personal data held about your child, this can be done through a subject access request. This is a formal procedure which is started in the first instance by contacting the Data Protection Officer of the College. The DPO will ensure that the personal data held is available for release within four weeks of the request being received by the College. The Data Controller will release the data either in paper form or if the request is made in electronic form then the data will be released in like manner if at all possible. If the data request is particularly complex then the four week period may be extended by a further four weeks but this will be made clear to the Data subject within the initial four weeks. The DC may request additional information to confirm the identity of the Data Subject or the legal means by which the person acting with Parental Responsibility is able to make a request. However, if the DC believes the Department of Education or the examination or assessment organisations hold personal data that you wish to review, (either because the data file has been transferred as a result of the student leaving DLS or due to other reasons) then the Data Subject will be advised to contact the data protection officer for these organisations should be contacted to initiate a subject access request process. (Please refer to Article 28 of the Data Protection Law, Jersey, 2018- for further information on the rights of the Data Subject.)

Right of rectification. If a Data subject or a person acting with parental responsibility, disputes the accuracy or completeness of personal data that is held by De La Salle College they may make a written request to the DC to rectify or change the personal data, stating the inaccuracy or explaining why the personal data is incomplete. The DPO will make reasonable efforts to verify this dispute over data. Following this process the DC will either authorise a change to the data or note on the data file that the Data subject disputes the data being held.

Right to Erasure. If a Data subject or a person acting with parental responsibility, makes a written request to the DC, then any personal data no longer necessary in relation to the purposes for which they were collected or otherwise processed will be erased without undue delay. Data retained as per Article 32 paragraph 3 of the Data Protection Law (Jersey) 2018, are not subject to the right to erasure.

The right to access personal data, Article 28 of the Data Protection Law (Jersey) 2018, does not apply to confidential references given by the DC. However, in the majority of cases the DC will inform the data subject of the contents of any reference provided so the Data subject can review the factual accuracy of the data it contains. Personal data is also except from Article 28 of the Data Protection Law (Jersey) 2018 in relation to data processed by a court or with respect to general Safeguarding as outlined in Article 61 of the Data Protection Law (Jersey) 2018.
The right to access personal data does not extend to information recorded by candidates during an examination, however the provisions of article 60 in relation to Examination marks will apply.
Please note that all rights under the Data Protection Law (Jersey) 2018 to do with information about your child rest with them as soon as they are old enough to understand these rights. This will vary from one child to another and you will wish to consider the position for your child, but, as a broad guide, it is reckoned that most children will have a sufficient understanding by the age of 13. We would therefore encourage you to share this note with your child if they are aged 13 or over.

This policy, the procedures related to it and its' practise are externally reviewed for compliance and the recommendations of the review will be acted on promptly.

Duties of the Data Controller (DC):

Article 6 of the Data Protection Law (Jersey) 2018 sets out the duties of the Data controller (DC) in some detail. However, a brief summary of these duties would be that the DC is:

- Responsible for compliance with the data protection principles provided in the law;
- Must ensure that appropriate safeguards are designed into the planning and implementing of personal data;
- Must comply with record keeping requirements;
- Must report any personal data breach;
- Must appoint a Data Protection Officer (DPO).

Duties of the Data Protection Officer (DPO)

Article 26 of the Data Protection Law (Jersey) 2018 sets out the duties of the Data Protection Officer (DPO) in some detail. However, a brief summary of these duties would be that the DPO is:

- Inform and advise the DC and the employees who carry out Data Processing of their obligations under the law;
- Monitor compliance with the law;
- Act as the contact point for the Data Protection Authority;
- Act as the contact point for the Data Subject or a person acting with Parental Authority for said Data Subject;
- Provide advice to the DC on the need for a conduct of data protection impact assessments;

The Right to Complain to the Data Protection Authority. Article 19 of the Data Protection Authority (Jersey) Law 2018 provides that any individual may make a complaint in writing to

the Authority in a form approved by the authority if the individual considers that the Data Controller has contravened or is likely to contravene the Data Protection (Jersey) Law 2018.

RETENTION SCHEDULES FOR COLLEGE RECORDS

Records in Series			Retention in school	Notes
	MANAGEMENT			
	1.1	School development plans	Permanent retention	
	1.2	Headteacher's personal filing	Current + 6 years	
	2. GOVERNING BODY			
	2.1	Instruments and Articles of Government	Permanent retention	
	2.2	Governor's Minutes, agendas and papers	Permanent retention	
	2.4	Proceedings of the PTA AGM	Permanent retention	
	2.5	Correspondence files	Current + 6 years	
	3. SCHOOL ORGANISATION			
	3.1	School prospectus	Permanent retention	
	3.2	Headteacher's official diary	Current + 1 year	
	3.3	Staff meetings Minutes	Current + 6 years	
	3.4	Administration and general files	Current + 10 years	
	3.6	Circulars to staff and pupils	Current + 2 years	
	3.7	Newsletters to parents	Permanent retention	
	3.8	Staff Handbook	Permanent retention	
	3.9	Visitors Book (VIP visitors)	Permanent retention	
	4.HEALTH & SAFETY			
	4.1	Health and Safety Policy statement	Current + 1 year	

	4.2	Staff Accident Records	Current + 6 years	
	4.3	Pupil Accident Records	DOB + 25	
	4.4	Safety incident report book	Current + 20 years	
	4.5	Maintenance log book	Current + 10 years	
	4.6	Training records	Current + 10 years	
	4.7	Health and Safety Reports	Permanent retention	

	4.8	Fire precautions log book	Current + 6 years	
	5.	**CHILD PROTECTION**		
	5.1	Child protection files	25 years post incident	
	5.2	Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Until the person's normal retirement age or 25 years from the date of the allegation, whichever is longer	
	6. PUPILS			
	6.1	Admission Registers (CMIS system)	Permanent retention	Admission registers are current while entries are being made and active until the pupil has left the school
	6.2	Failure to gain place	30 days from the commencement of the academic year.	
	6.3	Attendance Registers	Current + 3 years	
	6.4	Pupil's educational record/ file (CMIS)	Permanent retention	Remainder shredded at discretion of Department Manager
	6.5	Punishment books	Permanent retention	Transfer to Archive
	6.6	Absence books	Current + 6 years	

	6.7	Absence letters	Current + 2 years	
	7. STAFF			
	7.1	Staff personal files	Termination of employment + 3 years	
	7.2	Child Protection Files- any personnel files with allegations	100 years from end date of file	
	8. TEACHING			
	8.1	Curriculum development Minutes and files; Professional Development plan	Current + 6 years	
	8.2	School syllabus	Current	
	8.3	Timetables	Current + 6 YEARS	
	8.4	Record of homework set	Current	
	8.5	Teaching Aids (commercial and home-made)	Current	

	8.6	Examination results – held at DfESC	Permanent retention	
	8.7	Pupils' work	Current	
	9. FINANCE			
	9.1	Annual Budget	Permanent retention	
	9.2	Budget files	Current + 6 years	
	9.3	Headteacher's budget reports and budget monitoring tabulations	Current + 3 year	
	9.4	Annual statement of accounts	Permanent retention	
	9.5	Supplier Invoices	Current + 5 years	
	9.6	Delivery documentation	Current + 6 years	

	9.7	Invoices, bank account records, cashbooks, cash till rolls, debtor's records	Current + 5 years	
	9.8	Monthly Payroll	Current + 5 years	
	10. PROPERTY			
	10.1	Legal agreements, leases maintenance contracts	Current + 6 years	
	10.2	Contracts/Title Deed	Permanent retention	
	10.3	Register of tenders and quotations, orders for repairs, maintenance and supplies, records of letting school premises, maintenance log books, burglary, theft and vandalism report forms, contractors' reports	Current + 10 years	
	10.4	Records of insurance (policies and schedules)	Current	
	10.5	Plans	Permanent retention	
	11. EXTRA-CURRICULAR			
	11.1	School magazines	Permanent retention	
	11.2	Photographs	Permanent retention	
	11.4	Programmes – concerts, plays, sports day, lists of school prize winners etc	Permanent retention	
	11.5	School History	Permanent retention	One copy also to Jersey Library Ref. Section
	11.6	Audio-tape, video-tape recordings	Permanent retention	
	11.7	Record of school societies	Permanent retention	Minutes/ newsletters should be identified and preserved as far as possible