Data Protection Policy
(Abridged for Website)
January 2019

Carrigaline Community School
Waterpark,
Carrigaline,
Co. Cork.

T: 021 437 2300
E: info@carrigcs.ie

CIRCULATION SHEET

Client	Carrigaline Community School
Project Title	Carrigaline Community School GDPR Project 2018
Document Title	Data Protection Policy

Revisions				
Rev	**Status**	**Approved By**	**Office of Origin**	**Issue Date**
R01	Release	Ark Professional Consultancy Services www.arkservices.ie	Cork	15th Feb 2019

Circulation			
Name	**Organisation**	**Issue Date**	**Method**
Principal	Carrigaline Community School	15th Feb 2019	Email

TABLE OF CONTENTS

1 GDPR Compliance Statement

The characteristic spirit of Carrigaline Community School has at its core a desire to promote and protect the dignity of every member of its community, students, staff and parents. This includes respect for the protection of data stored at the school and for the right of access to this data. This policy is informed by these aspirations and also the General Data Protection Regulation of 2016 (GDPR). The policy applies to all school staff, the Board of Management, parents/guardians, students, (including prospective students) their parents/guardians, applicants for positions within the school and service providers with access to school data.

Carrigaline Community School is aware of its responsibilities as a controller of personal data under GDPR. The school has been briefed as to its scope and implications for our school. All members of staff at Carrigaline Community School 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.

As a school, we have always been committed to high standards of data protection, information security & privacy. Carrigaline Community School respects the privacy of students, staff and visitors to the school 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 an understanding of, and appreciation of 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. The Principal together with the Board of Management has overall responsibility for data protection at the school.

This policy requires the co-operation of all staff, visitors, contractors and others to enable Carrigaline Community School to discharge its responsibilities under the GDPR.

Carrigaline Community School 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 school 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: _____ Signed: _____

Chairperson of the Board of Management Principal

Date: _____2018 Date: _____2018

2 Scope

This policy states the commitment of Carrigaline Community School to comply with the EU GDPR as a Data Controller and with other relevant legislation. It applies to the personally identifiable information of EU residents such as staff, students, job applicants, and third parties communicating with Carrigaline Community School as Data Subjects under the purview of the GDPR.

It applies directly to functions of Carrigaline Community School 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 Carrigaline Community School.

3 Legal Obligations

In the addition to our obligations under GDPR, the implementation of this policy takes into account the school's other legal obligations and responsibilities in the Public Interest. Some of which are directly relevant to data protection:

- Under Section 9(g) of the Education Act, 1998, ensure that parents of a student, or in the case of a student who has reached the age of 18 years, the student, have access in the prescribed manner to records kept by that school relating to the progress of that student in his or her education;

- Under Section 20 of the Education (Welfare) Act, 2000, the school must maintain a register of all students attending the School;

- Under section 20(5) of the Education (Welfare) Act, 2000, a principal is obliged to notify certain information relating to the child's attendance in school and other matters relating to the child's educational progress to the principal of another school to which a student is transferring;

- Under Section 21 of the Education (Welfare) Act, 2000, the school must record the attendance or non-attendance of students registered at the school on each school day;

- Under Section 28 of the Education (Welfare) Act, 2000, the School may supply *Personal Data* kept by it to certain prescribed bodies (the Department of Education and Skills, the National Education Welfare Board, the National Council for Special Education, other schools, other centres of education) provided the School is satisfied that it will be used for a "relevant purpose" (which includes recording a person's educational or training history or monitoring their educational or training progress in order to ascertain how best they may be assisted in availing of educational or training opportunities or in developing their educational potential; or for carrying out research into examinations, participation in education and the general effectiveness of education or training);

- Under Section 14 of the Education for Persons with Special Educational Needs Act, 2004, the school is required to furnish to the National Council for Special Education (and its employees, which would include Special Educational Needs Organisers ("SENOs")) such information as the Council may from time to time reasonably request;

- The Freedom of Information Act 1997 provides a qualified right to access to information held by public bodies which does not necessarily have to be "personal data" as with data protection legislation. While schools are not currently subject to freedom of information legislation, if a school has furnished information to a body covered by the Freedom of Information Act (such as the Department of Education and Skills, etc.) these records could be disclosed if a request is made to that body;

- Under *Children First: National Guidance for the Protection and Welfare of Children* (2011) published by the Department of Children & Youth Affairs, schools, their boards of management and their staff have responsibilities to report child abuse or neglect to TUSLA - Child and Family Agency (or in the event of an emergency and the unavailability of TUSLA, to An Garda Síochána).

4 GDPR Principles

4.1 Principle 1: Lawfulness, fairness and transparency

Carrigaline Community School believes in operating our school fairly and ethically and this will extend to all personal data held for those purposes. 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. Advisory notices and privacy notices relating to data 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 Carrigaline Community School 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

Carrigaline Community School 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

Carrigaline Community School will make every effort to ensure that subjects' information is accurate and up to date. Carrigaline Community School will endeavour to ensure via appropriate levels of staff 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

Carrigaline Community School 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 replacing 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. Carrigaline Community School 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

Carrigaline Community School is responsible for, and is able to demonstrate compliance with GDPR. This means Carrigaline Community School 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

Carrigaline Community School 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;

Right of access requests must be responded to within one month through the Principal. See 12 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 12 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 the School / Department of Education to provide future services to you or to meet it statutory obligations for example under the National Archives Act, 1986.

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 a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, then the Data Controller must restrict processing to storage only whilst they consider whether their lawful basis for processing override the Rights and freedoms of the individual;
- 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, Carrigaline Community School will carry out an assessment of whether the data can be restricted without affecting the ability of the School / Department of Education to provide future services to you.

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 not apply if the decision;
- Is necessary for entering into or performance of a contract Is authorised by law;
- Is based on explicit consent;
- Does not have a legal/significant effect on the data subject.

At present there is no automated processing within the Department of Education.

6 Responsibilities

6.1 Board of Management

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;

In addition:

- Review and approve the Data Protection Policy;
- Supporting the Principal in the implementation of this policy;
- Review the implementation, effectiveness and compliance with policies, procedures and protocols;
- Ensure Data Protection Issues are an Agenda item at BOM meetings;
- Ensuring that personal data discussed at Board of Management Meetings is kept secure at all times;
- BOM Minutes are handed back to the Principal at the end of each BOM Meeting;

6.2 Senior Management including Principal & Deputy Principals

- Ensure the policy is communicated throughout the school;
- Ensure the policy is implemented throughout the school;
- Ensure personal data relating to students & staff is collected and processed in accordance with this policy;
- Ensure that the basic principles of data protection are explained to staff and parents/guardians. This will be done during staff induction, staff meetings and via the staff handbook.
- Ensure that there are regular updates to data protection awareness, so that data protection is a "living" process aligned to the school's ethos.
- Periodically check data held regarding accuracy.
- Driving privacy and data protection awareness in the school;
- Identifying training needs and arranging for refresher training sessions;
- Escalating appropriate issues to the Board of Management;
- 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) prior to any service provider being retained;
- Ensuring adequate assurances of GDPR compliance are obtained.
- Ensuring appropriate written contracts in place with all service providers;
- Ensure that Record-keeping of data protection items is carried out;
- Board of Management (BOM) Meetings:
    - Ensure BOM Minutes and records are kept secure in locked filing cabinets at all times;
    - Ensure that electronic versions of BOM Minutes are kept secure in password protected folders;
    - Ensure minutes that identifies vulnerable persons or particularly sensitive data is anonymized where possible.
    - Ensuring that BOM minutes are only distributed in paper copy and taken back following the completion of a meeting;
    - Ensure that information is kept secure at all times and that the information is shredded as soon as could be reasonably expected.
- Periodic reviews of all data protection arrangements are carried out.

6.3 Teaching Staff

6.3.1 General

- Read and sign acknowledgement of this policy;
- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Check that any information that they provide in connection with their employment is accurate and up to date;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. when entering notes about a student on any system);
- Ensure personal data is kept safe and secure, and is not disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Ensure personal data related to students is accurately processed in accordance with this policy;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion (e.g. if taking personal data to a TUSLA case conference to review a child, ensure the data are stored securely on an encrypted laptop);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with access requests.

6.3.2 Handwritten Notes / Paper Records

- Handwritten Notes can be lost or mislaid (whether in a journal or otherwise).
- Staff are urged to use the functionality provided on VS Ware and other school systems for taking records etc.
- Staff are advised that they have 4 options when taking handwritten notes:
    - If appropriate, the information on the note should be transferred to VS Ware, and the note shredded or,
    - Note is scanned and saved on the school's server in a secure folder, and the note shredded or,
    - Note is transferred to the students file in a secure filing cabinet in a locked office or
    - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy;
- Information required for Parent Teacher Meetings may be printed off VS Ware for that specific purpose providing that the teacher keeps that information secure at all times and that the information is shredded as soon as could be reasonably expected. Under no circumstances will teachers be permitted to take this information off the school premises.

6.3.3 Electronic Records

- When accessing school apps on their own mobile devices and or personal devices, staff will ensure these devices are pin protected, and passwords to school related apps are never saved / cached in the browser or app.
- Should your mobile device get lost / stolen, staff will immediately notify the Principal who will then ensure that login details are reset.
- Ensure that personal data is not visible to others (e.g. never display VS Ware on a projector or leave your computer when logged into VS Ware);
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure;
- When working with personal data, all staff must ensure that the screens of their computers / tablets / apps are always locked when left unattended;
- Never storing personal data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Only school supplied software is permitted for the recording of personal data at the school.

6.3.4 Emails

- Prepare emails with high levels of diligence and attention to detail i.e. Ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate;
- Limit identifying persons in emails / attachments where at all possible;
- Where emails and attachments contain sensitive personal information, staff are required to encrypt these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Encrypting emails where appropriate for other uses including the use of "Do Not Forward" etc.;
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Data should be encrypted before being transferred electronically where appropriate;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;

6.3.5 Records

- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;

6.3.6 Social Media

- Never sharing work-related data on unapproved systems (e.g. talking about a student in a teachers WhatsApp group);

6.3.7 Phishing / Malware

- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Never signing the School up to any apps or software relating to school business, or requiring students to engage with apps/software without the prior written approval of the Principal;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your VS Ware account etc);

6.4 Administrators

6.4.1 General

- Adhere to the values and standards set forth in this Policy, and comply with relevant school 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 data related to students, parents and staff is accurately processed in accordance with this policy;
- Keep the reception area clean and tidy;
- Ensure that personal data is not visible to others (e.g. leaving files on desk);
- Keep personal data out of sight of visitors to reception area;
- Ensure that their computer screen is not visible to visitors at reception;
- Diligence and attention-to-detail when entering data on to the School administrative system;
- Keep the data accurate, complete, and up-to-date;
- Ensuring filing cabinets and office door is kept locked when not in use;
- Prepare post with high levels of diligence and attention to detail. Ensuring that the correct letter is put in the correct envelope. Developing post protocol checklist (e.g. double-checking enclosures, envelope counts, etc);
- Keep anti-virus and anti-malware software up to date, install patches when required;
- 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 Principal if anyone attempts to obtain unauthorised access to personal data;

6.4.2 Subject Access Request

- Identify data subject requests when they are received (by letter, email etc). If received by telephone, asking the person to put their request in writing using the "Subject Access Request Form". Ensuring that all such requests (whether by phone, in person or by email or in writing) are immediately escalated to the Principal without delay;
- Being cautious about requests for information: where a request for personal data is received, asking the requester to verify their identity, ascertaining whether the requester is legally entitled to obtain the personal data;

6.4.3 Email

- Prepare emails with high levels of diligence and attention to detail i.e. Ensuring that the correct email address is entered; Using "bcc" instead of "to" field where appropriate; Encrypting emails where appropriate;
- If emailing to a group, verifying who the members of the group are;
- Be cautious and suspicious if an email asks you to click on links or open an attached document (even if from a familiar sender from a genuine email address);

6.4.4 Phishing / Malware

- Ensure that data are kept safe and secure. Use strong passwords (12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your VS Ware account etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering;

6.5 Year Heads

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. preparing summary assessments for teaching staff);
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Ensure only relevant teachers are provided with access to sensitive personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Staff are advised that they have 4 options when taking handwritten notes:
    - If appropriate, the information on the note should be transferred to VS Ware, and the note shredded or,
    - Note is scanned and saved on the school's server in a secure folder, and the note shredded or,
    - Note is transferred to the students file in a secure filing cabinet in a locked office or
    - If none of the above options are appropriate, then the note is destroyed / shredded as per the retention policy;
- School servers / cloud have been provided to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc. Staff are urged to use this infrastructure;
- Ensuring that at all times, Year Head Office & Filing Cabinets are locked when not in use.
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Ensure that disciplinary notes, behavioural reports etc. are never left on desks or in the staff room.
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.6 SEN Coordinator

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries (e.g. preparing summary assessments for teaching staff);
- Take all reasonable measures to secure sensitive personal information regarding students i.e. securing psychological assessments in secure filing cabinets, notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Where one page Individual Education Leaning Plans (IELP's) are prepared, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access. Ensure that the distribution of IELP's is done so securely;
- Use VS Ware ID No. to identify students in reports / files / relevant filing systems;
- Limit identifying persons in emails / attachments where at all possible;
- Where emails and attachments contain sensitive personal information, staff are required to encrypt the attachment to these emails i.e. ensuring only those with a password can open and access the contents of the email.
- Attachments containing personal data should be downloaded, stored securely, and then deleted;
- Staff will not save copies of personal data to their own computers, phones, tablets, USB sticks, Hard Drives;
- Ensuring that at all times, SEN Office & Filing Cabinets are locked when not in use.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Ensure only relevant teachers are provided with access to sensitive personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible (to ensure availability of data, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data (particularly sensitive personal data) is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.7 Guidance Counsellor

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries i.e. notes and record keeping;
- Take all reasonable measures to secure personal information regarding students i.e. securing notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Ensuring that the office and filing cabinets are locked when not in use.
- Where student files are online, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Where appropriate, ensure only relevant teachers are provided with personal information relating to a student;
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible (to ensure availability of data, allowing appropriate back-ups to be made, ensuring accountability, transparency, as well as keeping data safe and secure, etc);
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.8 Chaplain

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries i.e. notes and record keeping;
- Take all reasonable measures to secure personal information regarding students i.e. securing notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Ensuring that office and filing cabinets are locked when not in use.
- Where student files are online, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Where appropriate, ensure only relevant teachers are provided with access to personal information relating to a student;
- Diligence and attention-to-detail when entering data on the student's file (Data accurate, complete, and up-to-date);
- Ensure that any handwritten notes in any notebook are transferred to the students file as soon as possible;
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.

6.9 Caretaker

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Ensure the security of school buildings i.e. locking gates, locking doors;
- Ensure alarms are switched on each evening and working;
- Ensure that only authorised persons have access to School buildings;
- Storage of confidential wastepaper until it is securely shredded;
- Report any personal data breaches immediately to the Principal;
- Comply with and give assistance during audits, spot-checks, and inspections.

6.10 Adult Education Coordinator

- Adhere to the values and standards set forth in this Policy, and comply with relevant school procedures. Request clarification if there is uncertainty;
- Adherence to high standards of ethics and professionalism in all data entries i.e. notes and record keeping;
- Take all reasonable measures to secure personal information regarding Adult Education Programs & Attendees i.e. securing notes and records, ensuring your laptop or desktop computer is password protected and you log out each time you leave it;
- Ensuring that the office and filing cabinets are locked when not in use.
- Where student files are online, ensure that access to that folder(s) on the server is password protected to prevent unauthorised access.
- Remembering at all times that the person about whom you are writing may have the right to obtain copies of the data;
- Maintain up to date contact information
- Being suspicious: alert to possibility of impersonation, trickery, deception, phishing, social engineering etc.;
- Ensure personal data is never brought off-site unless appropriate steps are taken to protect the data in motion e.g. stored securely on an encrypted laptop;
- Never storing data relating to school business on unapproved devices or systems (e.g. personal smartphones, tablets, cloud storage accounts, usb sticks, hard drives etc.);
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) and change them regularly. Never share log-in credentials. Never allow someone else to see you entering passwords (particularly students!);
- Ensure passwords are unique (e.g. do not use the same password for your PayPal account as for your school account etc);
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;
- Assisting the Principal with subject access requests.
- Marketing Courses
    - Adult Education Department may from time to time market upcoming courses to previous attendees of similar / related courses;
    - Adult Education Coordinator must satisfy all GDPR requirements: lawful basis for processing (usually consent or legitimate interests), provision of fair processing information (transparency), appropriate technical and organizational measures to protect data;
    - Individuals have a specific right to refuse or opt out of Direct Marketing sent by the school; if based on consent, this can be withdrawn at any time;
    - Individuals must be informed of right to opt out, presented clearly and separately from other information on the registration forms;
    - Individuals must be able to opt out across all marketing channels;
    - Schools must honor opt out requests in a timely fashion, at no cost to the Individuals concerned;
    - Personal Data relating to that person must then be deleted unless retention strictly required.
    - Exceptions: necessary for establishment, exercise, or defense of legal claims, compelling legitimate grounds for continued processing outweighing privacy interests of the person.
    - If individuals request to opt out of direct marketing, the school should *suppress* rather than *delete* contact details: prevents re-acquiring details later and resuming Direct Marketing.

6.11 Website / Social Media Coordinator

- Exercise due care when posting photographs on the school's social media channels;
- Ensuring that photos are never shared on social media channels where consent has not been received from the student's parent / guardian;
- When posting photographs, using the student's first name only on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions.
- Deleting photographs off their personal device once emailed / posted on the school's social media channels;
- Use strong passwords (8-12 characters, mixture of alphanumeric, upper- and lower-case, and symbols e.g. %, £, & etc.) for all social media / website accounts and change them regularly. Never share log-in credentials i.e. same password for personal social media as school social media accounts.
- Immediately notify the Principal if anyone attempts to obtain unauthorised access to personal data;

6.12 Data Processors (Third Parties with whom the school share personal data)

- Process personal data only on documented instructions from the controller, including with regards to transfers of data outside the EEA;
- Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Take all measures pursuant to Article 32 on security of processing;
- Respect the conditions for enlisting another processor;
- 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;
- 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;
- At the choice of 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

Carrigaline Community School will ensure that management and staff 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 staff;
- A general email to all staff with the Data Protection Policy;

7.2 Balance of Rights

In using personal data for the operation of the school, 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

Carrigaline Community School 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

Carrigaline Community School 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 0.

7.5 Storage and Use of Personal Data

The security of personal data relating to students and staff is a very important consideration under the GDPR and is taken very seriously at Carrigaline Community School. Appropriate security measures will be taken by the school to protect unauthorised access to this data and to the data it is collecting and storing on behalf of the Department of Education and Skills (DES).

A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised staff 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 under password protected files;
- Any information which needs to be disposed of will be done so carefully and thoroughly;
- The premises at Carrigaline Community School are protected by a private security company and are monitored on a 24 hour/7 day week basis.

7.5.1 Paper based records

Paper based records shall be kept in a secure place where unauthorised people 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 folder on the school server / cloud or;
- 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 school supplied equipment / infrastructure i.e. school supplied desktop computers / laptops and school supplied servers, cloud storage;
- Data will be stored on designated drives and servers and will only be uploaded to approved cloud computing services.
- Servers containing personal data will be sited in a secure location.
- Data will be backed up frequently.
- All servers and computers containing data will be protected by approved security software and a firewall.

7.5.3 Use of Student Personal Data

We use student's personal data for purposes including:

- their application for enrolment;
- to provide them with appropriate education and support;
- to monitor their academic progress;
- to care for their health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.
- for the safety of our staff and students and for the protection of personal and school property (use of CCTV).

7.5.4 Use of Staff Personal Data

We use staff personal data for purposes including:

- their application for employment;
- to provide them with appropriate direction and support in your employment;
- to care for their health and well-being;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.;
- for the safety, health & wellbeing of other staff, students and visitors.

Carrigaline Community School understands that sensitive information may be identified through Garda Vetting. In the event that an employee's Garda vetting raises concerns, the information will be dealt with on a confidential basis. All information pertaining to such a situation will be stored in the same way as other data. The Board of Management/Board of Governors will not pass on a copy of a Garda Vetting Form to any other party.

7.6 Sharing Personal Data

From time to time, we may share personal data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc.

The sharing of student personal data and the nature of what is shared depends on various factors. The Government bodies to which we transfer personal data will use that data for their own purposes (including: to verify other information they already hold etc.) and they may aggregate it with other information they already hold about the data subject and the data subject's family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc). We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

7.7 Special Categories of Data

7.7.1 Children/Students

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Collect information on ethnic/cultural background of students with the consent of the parent/guardian for statistical analysis and reporting in aggregated format for the purposes of social inclusion and integration.
- Collect data on the religion of the student with the consent of the parent/guardian again for enrolment and statistical purposes.
- Process data related to health in respect of students with special educational needs or a disability for the purpose of ensuring that support services is made available to each child, as defined in section 2 of the Education Act 1998 including psychological services and a level and quality of education appropriate to meeting the needs and abilities of that person.

The Department of Education will only process special categories data relating to children or students for the purposes of allocating resources where this is provided for by way of enactment or the Constitution.

7.7.2 School Staff and Retired School Staff

Special categories of particularly sensitive personal information requires higher levels of protection. The school through the Department of Education may:

- Process data on trade union membership deductions with the consent of the staff member.
- Through the consent of the individual, process religious information where the individual wishes to be addressed by a religious title e.g. Father.
- Process information on sick leave but not the nature of the illness for the purpose of payments to school staff.
- Process data related to health where the occupational health service provides information in respect of applications for retirement on the grounds of ill health.
- Process data related to health when reviewing sample cases as part of an audit of public monies expended in the occupational health service.
- Process information related to religion where a person was or is part of a religious order and the processing of this data is required under the pension schemes.

7.7.3 Photographs of Students

The school maintains a database of photographs from school events held over the years. It has become customary to take photos of students engaged in activities and events in the interest of creating a pictorial as well as historical record of life at the school. Photographs and the student's first name only may be published on our school website, app, on social media or in brochures, yearbooks, newsletters, local and national newspapers and similar school-related productions.

Consent is requested from each parent when enrolling with the school. Should the parent wish to have his/her child's photograph removed from the school website, brochure, yearbooks, newsletters etc. at any time, we will duly comply on receipt of a written request to the school principal.

8 Data Processing Map & Retention Policy

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

Personal Data processed at Carrigaline Community School 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. Staff 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.

9 Data Privacy Notices

9.1 When is a Data Privacy Notice required?

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

- Where information is obtained from another source, a Data 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.

9.2 What needs to be included in a Data Privacy Notice ?

Data Privacy Notice s must contain specific information which informs data subjects of:

- Who is collecting the data;
- Why it is being collected;
- What legal basis is being relied upon to process the data;
- How it will be processed;
- How long it will be kept for;
- Who it will be disclosed to.

9.3 What rights people have in relation to their own data?

Individuals will also be made aware of their rights as per Section 5.

- 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.

10 Data Protection Communications

10.1 The Data Protection Policy

This document will be made known to all employees and staff as the primary source of Data Privacy Policy at Carrigaline Community School.

10.2 Carrigaline Community School Privacy Notice

Carrigaline Community School's main method of informing data subjects and the general public regarding our use of their data is the Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of Carrigaline Community School as the controller of personal information;
- 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 Carrigaline Community School;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Carrigaline Community School policy, and is not intended to constitute a contract with any person.

10.3 Carrigaline Community School Website Privacy Notice

Carrigaline Community School'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 Carrigaline Community School as the controller of personal information;
- 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 Carrigaline Community School;
- Summary technical details regarding information processing (including cookie use);

The Data Privacy Notice will be formatted appropriately for the medium in which it is published.

The Data Privacy Notice is considered an advisory notice regarding Carrigaline Community School policy, and is not intended to constitute a contract with any person.

10.4 Data Privacy and employees

Employees and contractors will be formally notified of Carrigaline Community School's position with respect to this policy via a staff briefing.

10.5 Communication plan for Privacy Notices

Carrigaline Community School will ensure that staff 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.

Carrigaline Community School's main vehicle for informing the public of our privacy policy is the data privacy notice which is published on our website. This will be revised as necessary to ensure compliance.

Where certain classes of users (e.g. students) need to be informed more proactively regarding our use of their personal data, we will accomplish this by direct email to those users. 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 data Privacy Notice itself contains an advisory to users to check regularly for changes.

11 Third Parties

11.1 General

Carrigaline Community School avails of the services of outside parties who act as Data Processors on our behalf to assist us in essential school processes.

These include but are not limited to software providers & IT contractors.

Carrigaline Community School 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 Carrigaline Community School Data Protection Policy;
- A Data Processing Agreement is 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.

11.2 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 school processes. Carrigaline Community School warrants that the use of non-EEA services is a school necessity. In these cases, Carrigaline Community School has identified the following:

Processor	Stored in the EU/EEA?	EU/US Privacy Shield Agreement in place
G Suite	Not always	Yes
VS Ware	Yes	N/a
ESI Net	Yes	N/a
Host Dime UK	Yes	N/a

12 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, Carrigaline Community School 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, Carrigaline Community School will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, Department of Education 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, Carrigaline Community School 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 data processor must be reported to Carrigaline Community School as soon as the data processor becomes aware of the incident.

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 school 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 Carrigaline Community School will report the incident to the DPC.

Carrigaline Community School 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 may be by email (preferably), telephone or fax and must not involve the communication of personal data. 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 school to provide a detailed written report of the incident, Carrigaline Community School 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 school has not already done so. If necessary, the DPC may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

Even where there is no notification of the DPC, Carrigaline Community School 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 school did not consider it necessary to inform the DPC. Such records should be provided to the DPC upon request.

12.1 Data Breach Action Plan

12.1.1 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;

12.1.2 Containment and Recovery

- Establish who within the school 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);

12.1.3 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;

12.1.4 Notification

- On the basis of the evaluation of risks and consequences, the Principal Team will decide whether it is necessary to notify relevant stakeholders i.e.
    - the Gardaí;
    - the Data Subjects affected by the breach;
    - the Data Protection Commissioner;
    - the School'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 school 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 school's policy on Data Breach above, and where there is any doubt, legal advice will be sought.

12.1.5 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 staff.

13 Subject Access Requests (SARs)

Carrigaline Community School recognises the right of data subjects to request information regarding data we hold on them.

13.1 Student making a Subject Access Request

- A student aged eighteen years or older (and not suffering under any medical disability or medical condition which may impair his or her capacity to give consent) may give consent themselves;
- If a student aged eighteen years or older has some disability or medical condition which may impair his or her ability to understand the information, then parental/guardian consent will be sought by the school before releasing the data to the student;
- While a student aged from thirteen up to and including seventeen can be given access to their personal data, depending on the age of the student and the nature of the record, i.e. it is our policy that:
    - If the information is ordinary, routine or non-controversial (e.g. a record of a test result) the student could readily be given access;
    - If the information is of a sensitive nature, parental/guardian consent will be sought before releasing the data to the student;
    - If the information would be likely to be harmful to the individual concerned, parental/guardian consent will be sought before releasing the data to the student;
- Each student request for Access to Personal Data will be assessed individually.

13.2 Parents making a Subject Access Request

Where a parent/guardian makes an access request on behalf of his/her child (a student aged under 18 years), the right of access is a right of the data subject (i.e. it is the student's right). In such a case, the access materials will be sent to the child, not to the parent who requested them. This means that the access request documentation will be sent to the address at which the student is registered on the school's records and will be addressed to the student subject to the provisions above.

13.3 Third Parties making a Subject Access Request

The purpose of a SAR is to make individuals aware of and allow them to verify the lawfulness of the processing of their personal data. Under the GDPR, individuals have the right to obtain confirmation as to whether personal data is being processed. If personal information is being processed, they are entitled to access the following information:

- the reasons why their data is being processed,
- the description of the personal data concerning them,
- anyone who has received or will receive their personal data, and
- details of the origin of their data if it was not collected from them.

13.4 Data Subject Rights

Data Subjects are entitled to obtain, based upon a request made in writing to Carrigaline Community School 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.

13.5 Logging Subject Access Requests

All requests received for access to or rectification of Personal Data must be directed to the Principal, who will log each request as it is received using the Subject Access Request Register. The data subject will be asked to fill out the Appendix 1: Subject Access Request Form.

13.6 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 Carrigaline Community School to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Carrigaline Community School cannot respond fully to the request within 30 days, the school 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 Carrigaline Community School individual who the Data Subject should contact for follow up.

13.6.1 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.

14 Disposal of Personal Data

Carrigaline Community School will conduct a regular review of the personal data we hold for the purpose of disposing of redundant personal data. Such a review will take place on an annual basis and will 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 0);
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 0);
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 0.
    b. Identifying the records for disposal.
    c. Obtain permission from the Principal to dispose of the records.
    d. Document the disposal of records.
4. Suitable third-party service provider should be contacted to provide a secure erasure and destruction service i.e. confidential shredding through a certified data destruction specialist.
5. Consultation should also take place with the Principal for advice on record retention periods and to ensure that records are disposed of in a safe, secure and appropriate manner.

15 Governance framework

15.1 Supervisory Authority

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

15.2 Monitoring Compliance

Carrigaline Community School will carry out internal GDPR compliance audits against school 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 Carrigaline Community School 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 & Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

The Data Protection Coordinator, in cooperation with key stakeholders will devise a plan with a schedule for correcting any identified gaps within a defined and reasonable time frame.

15.3 Disciplinary Procedure

Breaches of the GDPR or the school's 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 Principal in accordance with the School's 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.

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 Carrigaline Community School

Are you a current/former* member of staff?	**YES / NO**
If yes, please provide the following details: Period which you were an employee in Carrigaline Community School i.e. Month & Year.:	
Are you a current/former student of Carrigaline Community School?	**YES / NO**
If yes, please provide the following details: Period which you were a student in Carrigaline Community School i.e. Final Year.:	
If neither a student / employee, please indicate your relationship with the Carrigaline Community School 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 Carrigaline Community School 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**
- **Copy of bank statement**
- **Staff/student ID Card**
- **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 data 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: **Reception** **Carrigaline Community School** **Waterpark, Carrigaline, Co. Cork.** **T: 021 4372300** **E: Info@carrigcs.ie**

FOR SCHOOL USE ONLY:

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

Privacy Notice for the Data Subject Access Request

The purposes for which the school 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;

Further Processing:

- Where the Department intends to further process your data for a purpose other than the purposes listed above, the Department will provide you prior to that further processing with information on that other purpose and with any relevant further information on the processing activity and your data protection rights;

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;

Rights

- You may also exercise your right to correct your data, seek to restrict how it may be processed or object to how it may be processed. Your data will not be used for automated decision-making or profiling, see http://gdprandyou.ie/wp-content/uploads/2018/03/Rights-of-Individuals-under- the-General-Data-Protection-Regulation.pdf;
- While you have a right to have your data or that of your child deleted the Department may not be able to agree to your request if it is less than 3 years since you submitted your application;
- You have the right to lodge a complaint with the Data Protection Commissioner, please see www.dataprotection.ie;

Contact Details

- Carrigaline Community School is the data controller for the processing of your data. If you have any query in respect of this you may contact the Principal or by post to Carrigaline Community School, Waterpark, Carrigaline, Co. Cork.

Appendix 2: Website Data Privacy Notice (effective 25th May 2018)

This Privacy Notice governs the manner in which Carrigaline Community School collects, uses, maintains and discloses information collected from users (each, a "User") of the https://www.carrigcs.ie website ("Site"). This Privacy Notice applies to the Site and our school.

Personal Identifiable Information (Post Primary Students)
We collect personal identifiable information from prospective students in a variety of ways in connection with the delivery of education at our school. We will collect personal identifiable information from data subjects when they voluntarily submit such information to us:

Post Primary Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; PPS Number; Address; Nationality; Birth Certificate; Medical Conditions; Programme Subjects & Courses Exemptions; Medium of learning Irish/English; Psychometric Testing Results (where applicable); Religion; Psychological Assessment Results (where applicable); Book Rental Scheme; Transportation Scheme;
- Parent / Guardian Name; Phone Number; Home address; Mobile Number; Emergency Contact Person & No., Email, Mothers Maiden Name; Family Members (current / past); Medical Card;
- Name, Address & Tel. No. of GP, Previous Educational History.
- Photos with classmates, tours, matches, awards etc.
- CCTV Images.
- Classroom based assessments and exam results;
- State Examination Results;

How we use collected information

We use your personal data for purposes including:

- your application for enrolment;
- to provide you with appropriate education and support;
- to monitor your academic progress;
- to care for your health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

Personal Identifiable Information (Teaching Staff)
We collect personal identifiable information from prospective staff & staff in a variety of ways in connection with the delivery of education at our school. We will collect personal identifiable information from data subjects when they voluntarily submit such information to us:

Staff & Prospective Staff Data (Lawful Basis: Public Interest, Consent, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payroll No.;
- Teaching Council Registration No.;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions e.g. trade union subscription;
- 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 (staff) 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 process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

Personal Identifiable Information (Adult Education Tutors)
We collect personal identification information from tutors and prospective tutors in a variety of ways in connection with their employment at our school.

Tutor's Personal Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payment details;
- Service history;
- 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 etc.;

How we use collected information
We use your personal data for purposes including:

- your application to become a tutor for one of our Adult Education courses;
- to provide you with appropriate direction and support;
- to care for your health and well-being;
- to process payroll and comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- to process appeals, resolve disputes, and defend litigation etc.

Personal Identifiable Information (Adult Education Students)
We collect personal identification information from adult education students in connection with the delivery of education at our school.

Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; Address; PPS Number; Phone Number;
- Photos with classmates, awards etc.
- CCTV Images.

How we use collected information
We use your personal data for purposes including:

- your application for enrolment on our adult education course;
- to provide you with appropriate education and support;
- to monitor your progress;
- to care for your health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- 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 post primary & adult education students, this generally means we will retain data for up to 7 years after a student has left the school,

For staff we will retain data for the duration of employment and up to 7 years thereafter. If you apply for a position but you are unsuccessful, will retain your data for up to 18 months.

After this time, your data will be destroyed by confidential shredding our deletion from our school's database.

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

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners, Solas as appropriate etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

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 or a new school 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 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 Users means of connection to our Site, such as the operating system and the Internet service providers utilized and other similar information.

Third party websites
Users may find advertising or other content on our Site that link to the sites and services of our partners, suppliers, advertisers, sponsors, licensors and other third parties. We do not control the content or links that appear on these sites and are not responsible for the practices employed by websites linked to or from our Site. In addition, these sites or services, including their content and links, may be constantly changing. These sites and services may have their own privacy policies. Browsing and interaction on any other website, including websites which have a link to our Site, is subject to that website's own terms and policies.

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 aboutcookies.org). 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 Carrigaline Community School 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.

Compliance with children's online privacy protection act
Protecting the privacy of the very young is especially important. For that reason, we never collect or maintain information at our Site from those we actually know are under 13, and no part of our website is structured to attract anyone under 13.

Changes to this privacy policy
Carrigaline Community School has the discretion to update this privacy policy at any time. When we do, we will revise the updated date at the bottom of this page. 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.

How to contact us
For general queries and requests of any kind, please contact:

Principal
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

Appendix 3: Carrigaline Community School
Email Data Privacy Notice
(for inclusion in all email signatures)

Example (in bold below for effect):

Best regards,

Principal
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

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 in the Public Interest. For more information please review our Privacy Notice here.

Appendix 4: Carrigaline Community School Enrolment Form Privacy Notice (effective 25th May 2018)

Who is collecting the data
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

This Privacy Notice governs the manner in which Carrigaline Community School collects, uses, maintains and discloses information collected using School Forms.

Personal Identifiable Information (School)
We collect personal identification information from students & prospective students in a variety of ways in connection with the delivery of education at our school. We will collect personal identification information from data subjects only if they voluntarily submit such information to us:

Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; PPS Number; Address; Nationality; Birth Certificate; Medical Conditions; Programme Subjects & Courses Exemptions; Medium of learning Irish/English; Psychometric Testing Results (where applicable); Religion; Psychological Assessment Results (where applicable); Book Rental Scheme; Transportation Scheme;
- Parent / Guardian Name; Phone Number; Home address; Mobile Number; Emergency Contact Person & No., Email, Mothers Maiden Name; Family Members (current / past); Medical Card;
- Name, Address & Tel. No. of GP, Previous Educational History.
- Photos with classmates, tours, matches, awards etc.
- CCTV Images.
- Classroom based assessments and exam results;
- State Examination Results;

How we use collected information
We use your personal data for purposes including:

- your application for enrolment;
- to provide you with appropriate education and support;
- to monitor your academic progress;
- to care for your health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- 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 students, this generally means we will retain data for up to 7 years after a student has left the school. After this time, your data will be destroyed by confidential shredding our deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Carrigaline Community School Data Protection Policy which is available to you on request.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

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 or a new school 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: Carrigaline Community School
Staff Privacy Notice
(effective 25th May 2018)

Who is collecting the data
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

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

Personal Identifiable Information
We collect personal identification information from staff and prospective staff in a variety of ways in connection with your employment at our school.

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

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payroll No.;
- Teaching Council Registration No.;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions e.g. trade union subscription;
- 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 (staff) 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 process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- 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 our deletion from our school's database.

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

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the State Examinations Commission, the Department of Education and Skills, NCSE, TUSLA, An Garda Síochána, HSE, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes (including: to verify other information they already hold about you, etc) and they may aggregate it with other information they already hold about you and your family. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

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 or a new school 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 6: Carrigaline Community School
Adult Education Tutor's Privacy Notice
(effective 25th May 2018)

Who is collecting the data
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

This Privacy Notice governs the manner in which Carrigaline Community School collects, uses, maintains and discloses information collected throughout the recruitment, hiring and employment of tutors in our Adult Education Department.

Personal Identifiable Information
We collect personal identification information from tutors and prospective tutors in a variety of ways in connection with their employment at our school.

Tutor's Personal Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Payment details;
- Service history;
- 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 etc.;

How we use collected information
We use your personal data for purposes including:

- your application to become a tutor for one of our Adult Education courses;
- to provide you with appropriate direction and support;
- to care for your health and well-being;
- to process payroll;
- to comply with our legal obligations as an employer;
- to comply with our monitoring and reporting obligations to Government bodies;
- 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 tutors 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 and deletion from our school's database.

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

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the Solas, HSE, the Department of Social Protection, the Revenue Commissioners etc.

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 or a new school 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 7: Carrigaline Community School
Adult Education Enrolment Form Privacy Notice
(effective 25th May 2018)

Who is collecting the data
Carrigaline Community School
Waterpark, Carrigaline, Co. Cork.
T: 021 4372300
E: Info@carrigcs.ie

This Privacy Notice governs the manner in which Carrigaline Community School collects, uses, maintains and discloses information collected using School Forms.

Personal Identifiable Information
We collect personal identification information from adult education students in connection with the delivery of education at our school.

Student's Data (Lawful Basis: Public Interest, Consent, Legal Obligation):

- Name; Surname; Date of Birth; Address; PPS Number; Phone Number;
- Photos with classmates, awards etc.
- CCTV Images.

How we use collected information
We use your personal data for purposes including:

- your application for enrolment on our adult education course;
- to provide you with appropriate education and support;
- to monitor your progress;
- to care for your health and well-being;
- to care for our staff and students;
- to process grant applications, fees and scholarships;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an education body;
- to comply with our monitoring and reporting obligations to Government bodies;
- 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 adult education students, this generally means we will retain data for up to 7 years after a student has finished the course. After this time, your data will be destroyed by confidential shredding or deletion from our school's database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in Carrigaline Community School Data Protection Policy which is available to you on request.

Sharing your personal information
We do not sell or trade personal identification information to others. We may share your data with the Solas, the Department of Social Protection, the Revenue Commissioners etc.

The level of sharing and the nature of what is shared depend on various factors. The Government bodies to which we transfer your personal data will use your personal data for their own purposes. We also share your personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc), We are legally required to provide certain records relating to the progress of a student (under 18 years) in his/her education to the student's parents/guardians, including results of examinations.

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 or a new school 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.

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									
15									

Acknowledgement of the Data Protection Policy

I wish to acknowledge receipt of the Data Protection Policy.

Date	Employee Signature	Blocks