Chenderit School
A VISUAL ARTS COLLEGE
aim high

CHENDERIT SCHOOL
DATA PROTECTION POLICY

REVIEWED BY GOVERNING BODY May 2018
ADOPTED BY GOVERNING BODY May 2018

Responsibility: It is the responsibility of the Governors to ensure procedures are in place to ensure that the school complies with the General Data Protection Regulations (GDPR) 2016

Contents:

1. Introduction

In order to operate efficiently Chenderit School [the School] has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, students, parents/carers, contractors, third parties and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is committed to ensuring personal information is properly managed and that it ensures compliance with the General Data Protection Regulations (GDPR) 2016. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

2. Scope

This policy applies to all employees, governors, parents/carers, contractors, third parties, agents and representatives and temporary staff working for or on behalf of the School.

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The GDPR does not apply to access to information about deceased individuals.

This policy does not operate in isolation but links to other school policies such as, Child Protection and Safeguarding, ICT Acceptable Use and CCTV System.

3. Responsibilities

The Governors have overall responsibility for compliance with the GDPR.

The Data Protection Officer, on behalf of the Headteacher (the Data Controller), is responsible for ensuring compliance with the GDPR and this policy within the day to day activities of the School. The Data Protection Officer, on behalf of the Headteacher, is responsible for ensuring that appropriate training is provided for all staff.

All members of staff, governors, agents, representatives or contractors who hold or collect personal data are responsible for their own compliance with the GDPR and must ensure that personal information is kept and processed in-line with the GDPR.

4. The Requirements

Article 5 of the GDPR stipulates that anyone processing personal data must comply with six principles which set out the main responsibilities for organisation. The principles require that personal information shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

GDPR also require that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Personal data meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

Special categories of personal data is personal data consisting of information such as the following:-

- the racial or ethnic origin of the data subject,
- political opinions
- religious beliefs or other beliefs of a similar nature
- biometrics
- physical or mental health or condition

5. Notification

The General Data Protection Regulations (GDPR) 2016 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School is registered.

The School will review the Data Protection Register (http://www.ico.gov.uk/ESDWebPages/search.asp) annually, prior to renewing the notification to the Information Commissioner.

6. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following:

- The identity of the data controller, e.g. the School;

- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- Who the information will or may be shared with; and
- How to contact the data controller.

This must be at the time that information first starts to be gathered on an individual.

7. Conditions for Processing

Processing of personal information may only be carried out where one of the conditions of Article 6 of the GDPR has been satisfied.

Processing of sensitive personal data may only be carried out if a condition in Article 9 is met as well as one in Article 6.

8. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- *other members of staff on a need to know basis;*
- *relevant Parents/Carers;*
- *other authorities if it is necessary in the public interest, e.g. prevention of crime;*
- *other authorities, such as the LA and schools to which a pupil may move, where there are legitimate requirements (*The Education (Pupil Information) (England) Regulations 2005) *covers Data Protection issues and how and what information should be transferred to other schools.*

The School should not disclose anything on a pupil's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict advice should be obtained from The Information Commissioner's Office (ICO).

When giving information to an individual it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

9. The individual's right to access their personal information (Subject Access Requests)

Any person whose details are held by the School is entitled, under the GDPR, to ask for a copy of all information held about them (or child for whom they are responsible).

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one calendar month. For schools, this is excludes school holiday

weeks, where we reserve the right to add the number of school holiday weeks onto the timescale.

Subject access requests must be provided free of charge. However, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

10. Provision of data to children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 13 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

11. Parents' rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2005 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records.

12. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

Full details of information security for IT can be found in our IT Security Policy and its associated documents. The basis of which includes password protection, encrypted devices, screensavers and off-site back-up discs.

13. Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined (see Appendix A – Retention Schedule)

14. Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

15. Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give written consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

16. Photographs

Whether or not a photograph comes under the GDPR is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children.

17. Breach of the policy

Non-compliance with the requirements of the GDPR by employees, governors, parents/carers, contractors, third parties, agents and representatives and temporary staff working for or on behalf of the School could lead to serious action being taken by third parties against the school authorities. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

Non-compliance by employees, governors and temporary staff working for or on behalf of the School is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal.

Abbreviations

Abbreviation	Description
GDPR	General Data Protection Regulations 2016
EIR	Environmental Information Regulations 2004
FoIA	Freedom of Information Act 2000

Glossary

Data Controller	A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in paper files.
Data Subject	The individual who the data or information is about
Educational record	The educational record is confined to information that comes from an employee of a school, the pupil or their parents. Communications about a particular child from staff at a school may therefore form part of that child's official educational record, as may correspondence from other professionals engaged to provide prescribed services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a member of staff solely for their own use does not form part of the official educational record.
Information Commissioner	The independent person who has responsibility to ensure the GDPR is complied with. They can advise on data protection issues and can enforce measures against individuals or organisations who do not comply with the GDPR.
Notified Purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.
Personal Data	'personal data' defined in Article 4 of GDPR means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Processing	'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
Processed fairly and lawfully	Data must be processed in accordance with the 3 provisions of the GDPR. These are the data protection principles, the rights of the individual and notification.

Special categories of personal data	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Subject Access Request	An individual's request for personal data under the General Data Protection Regulations (GDPR) 2016

Extracted from Article 6 of the General Data Protection Regulations 2016 on 01/05/18

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose

limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific L 119/36 EN Official Journal of the European Union 4.5.2016 processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation

Extracted from Article 9 of the General Data Protection Regulations 2016 on 01/05/18

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or

Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.