CRANSLEY SCHOOL

CRANSLEY SCHOOL

Data Protection Policy

Seeking Excellence | Nurturing Relationships | Venturing Beyond

Policy Reviewed: November 2019

Policy Ratified by Governors: December 2019

Next Review Date: December 2020

CRANSLEY SCHOOL

Document Control

Date	Author	Version	Comment
10/02/2018	W Crumpton	1st draft	
15/02/2018	W Crumpton	Extended 1st draft	Discussed with N Willetts, sanction to complete draft.
27/02/2018	W Crumpton	Completed 1st draft	To be discussed with Governors 01/03/2018.
03/03/2018	W Crumpton	2nd draft	Update post meeting with General Purposes Committee
16/03/2018	W Crumpton	3rd draft	Amendments post GDPR Training Course
22/03/2018	W Crumpton	4th draft	Amendments post General Purposes Committee meeting 21 March 2018.
26/04/2018	W Crumpton & N Willetts	5th draft	Final draft agreed by Governors before posting on website.
03/06/2019	W Crumpton	6th draft	Update following the implementation of the Data Protection Act 2018
28/06/2019	W Crumpton	7th draft	Update following the update of Working Together to Safeguard Children
25/10/2019	W Crumpton	8th draft	Update following the September 2019 revision of KCSiE re safeguarding and sharing information.

CRANSLEY SCHOOL

CRANSLEY SCHOOL

General statement of the duties of Cransley School.

From May 2018 the protection of persons with regard to the processing of personal data and the free movement of such data is governed by EU Regulation 2016/679, generally known as the General Data Protection Regulation (GDPR). Along with the Data Protection Act 2018 (DPA), the UK data protection regime takes a flexible risk-based approach to the use and security of personal data..

The GDPR is concerned with the rights of individuals to gain access to personal information held about them by an organisation or individual within it and the right to challenge the accuracy of data held. It relates to data held in any form, including written notes and records, not just to electronic data. The GDPR and DPA extend the scope of previous data protection laws to include: genetic data and biometric data where processed to uniquely identify an individual; on-line identifiers (e.g. IP address); and personal data that has been pseudonymised (e.g. key-coded).

Cransley School Ltd (the school) is a private company limited by guarantee and the **data controller** as defined in the GDPR. This policy applies to personal information held and processed by Cransley School Ltd, and sets out its duties under the GDPR and DPA, including the duties of its staff. It provides guidance on processing, retaining, security and disposal of all personal data held by Cransley School

Cransley School is required to process personal data regarding pupils, their parents or guardians and staff as part of their operation, and shall take all reasonable steps to do so in accordance with this Policy and the principles of the GDPR.

The school aims to have transparent systems for holding and processing personal data. Any reference to personal data in this policy includes reference to "special categories" of personal data[1]. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

Any individual is entitled to request access to information relating to their personal data held on a relevant filing system by the school. A relevant filing system is any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Personal data can be held in any format (electronic, paper-based, and photographic) from which the individual's data can be readily extracted

In this policy any reference to pupils includes current, past or prospective pupils.

The General Data Protection Regulation

Although the GDPR is a Regulation made by the European Union(EU) and The UK is negotiating a departure from the EU, The UK government has confirmed that the GDPR will apply in full to the processing of data in the UK.

GDPR defines '*processing*' as "*any operation or set of operations which is performed on 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".*

With respect to Cransley School, **processing** personal data relates to the collection and storage of personal data so as

[1] The term "*sensitive personal data*" was used in previous legislation. The GDPR refers to this type of data as "*special categories of personal data*". The latter are broadly the same as the earlier categorybut include, in addition, genetic data and biometric data where processed to uniquely identify an individual. Personal data referring to criminal convictions and alleged offences are not classed as special categories of personal data by the GDPR, but similar safeguards apply to its processing.

to enable it to carry out the day-to-day functions of a school. It includes obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data for the purposes of; employing staff with the associated legal duties, compliance with other legal duties such as safeguarding of pupils, and to enable the school to contact parents and alumni with information of interest to them, to promote the activities of the school and celebrate the successes of pupils.

Processing also includes transferring data to 3rd parties (see separate section below).

The GDPR applies to information relating to both "**personal**" and "**special categories**" of personal data.

Personal data means any information relating to a living individual person (data subject) who can be identified from that information (or from that data and other information in possession of Cransley School). The school may process a wide range of personal data of pupils, their parents or guardians and staff, as part of their operation. To qualify as personal data, the data must allow the identification of, and give information relating to, a data subject. Personal data includes facts and any expression of opinion about an individual. Examples of personal data are: names and addresses; bank details; academic, disciplinary, admissions and attendance records; references; and examination scripts and marks.

Special categories of personal data are defined in the GDPR as information in respect of; racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or orientation.
They also include ; genetic data and biometric data where processed to uniquely identify an individual.
Personal data referring to criminal convictions and alleged offences are not classed as special categories of personal data by the GDPR, but similar safeguards apply to its processing.
Special categories of personal data can only be processed under strict conditions, including a condition requiring consent of the person concerned to such processing.

In order to comply with the GDPR the school must the process personal data in accordance with the following **principles**:

Principle 1: Personal data shall be processed fairly and lawfully and in a transparent manner.

The collection and disclosure of data is only lawful if it meets at least one of the following criteria (Article 6 GDPR):

• With the consent of the data subject for one or more specific purposes; or,

• In performance of a contract (for example to process an application as part of the admissions process); or,

• If there is a legal obligation (for example under employment law or for tax purposes); or

• For the protection of the vital interests of the individual (for example to prevent injury or other damage to the health of the data subject), or,

• In the legitimate interest of the data controller, unless it is prejudicial to the interests of the individual (for example for the purpose of equal opportunities monitoring).

Personal data must meet all of the following criteria in order to be processed fairly:

• It should be transparent to individuals what personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data will be processed.

• Data will only be collected from persons who have the authority to disclose it. If personal information is collected from a third party the data subject will be informed of the use and origin of the information (Article14 GDPR).

• Any information and communication relating to the processing of those personal data must be easily accessible and easy to understand, and that clear and plain language be used.

• Individuals should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to such processing.

• Subjects must not be deceived or misled in any matter related to the use of personal data.

In addition to the requirements outlined above, Special categories of personal data may only be processed if it also meets at least one of the following criteria (Article 9 GDPR):

• The data subject has given explicit consent.

• It is necessary to meet requirements of employment law.

• It is necessary to protect the vital interests of the subject or another person i.e. if the situation is a matter of life or death.

• It is carried out in the course of the legitimate activities of the data controller (e.g. in order to conduct a business), with appropriate safeguards.

• The data subject has already manifestly made the information public.

• It is necessary for legal proceedings, obtaining legal advice or defending legal rights.

• It is necessary for reasons of substantial public interest.

• It is necessary for medical purposes.

• It is necessary for reasons of public health.

• It is necessary in order to comply with legislation from the Secretary of State.

Personal data relating to criminal convictions may only be processed if authorised by law, providing appropriate safeguards are applied to ensure the rights and freedoms of the data subject.

Principle 2: Personal data will be obtained only for one or more specified and lawful purposes.

Data will not be further processed in any manner incompatible with the initial specified purpose or those purposes for which it was obtained. To satisfy the first principle (fair processing) the data subject(s) must not have been misled or deceived as to the reason(s) for processing.

Principle 3: Data must be adequate, relevant and not excessive.

Personal information, which is not necessary for the intended processing, must not be acquired, i.e. personal information cannot be collected just because 'it may be useful'.

Principle 4: Data must be accurate and up to date.

Cransley School must ensure that there is a system in place to review data for accuracy and to ensure that it is up to date. Procedures must be in place to make any amendments requested by a data subject, or a record kept if the amendment is not considered appropriate.

Principle 5: Data must not be kept for longer than required for the purpose.

Cransley School must indicate the length of time that data is to be in use and archived for any given purpose. This time period must be seen as justifiable for the particular purpose and in line with any legislation covering the processing.

Information should not be kept any longer than the time period indicated to the data subject.

The school must regularly review data held in order to assess whether information is still required and to ensure information is retained only for as long as is necessary. GDPR expects time limits on retention to be established by the data controller (GDPR " Recital" 39).

The school will implement a disposal policy to which all staff can refer when they need to dispose of personal information. A disposal record will assist the school in responding to enquiries made under the GDPR.

Before disposing of any data the school will consider the following key points:

• Any legal requirements (e.g. possible negligence action).

• The length of any appeals procedure relating to the information.

• The number of times in the last two or three years that a particular type of record has been accessed.

Principle 6: Data must be processed in line with individual's rights

This is strongly linked to the first principle of fair and lawful processing. Data subjects have the right to know details of the processing and the right of access to personal information. Accordingly, at the time the data is obtained the data subject should be provided with the following information:

- the identity and the contact details of the controller;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the legitimate interests of the school for which the data is processed.

Data subjects have the following rights:

• The right of **access** to the data to confirm;

- the nature of the data, including a copy of the data,
- the purpose of the processing,
- where possible the envisaged period for which the data will be stored and,
- where the data was not collected from the subject, any available information as to its source.

See the section below on obtaining access to personal data.

• The right to **rectification**; to correct, without undue delay, the rectification of inaccurate data, and to have incomplete data completed (Article 16 GDPR).

• The right of **erasure** (Article 17 GDPR); to the erasure without delay where:

- processing the data is no longer necessary,
- the subject withdraws consent,
- the subject objects to the processing (see the right to object below),
- the data have been unlawfully processed,
- the data has to be erased to comply with a legal obligation.

• The right to the **restriction of processing** where; the accuracy of the data is contested, processing is unlawful, or the data subject has objected to processing (Article 18 GDPR).

Data controllers must communicate any rectification, erasure or restriction of processing to the data subject and to any person to whom the data has been disclosed.

• The right to **data portability** (Article 20 GDPR); to have data provided to one data controller passed to another controller without hindrance (this is unlikely to apply to data controlled by the school).

• The right to **object** to data processing (Article 21 GDPR). The controller must comply with such an objection unless he demonstrates compelling legitimate grounds for the processing which overrides the interests, rights, and freedoms of the data subject or for legal reasons. (This right also relates to direct marketing which is not an issue that affects Cransley School[2]).

• The right to **lodge a complaint with the supervisor authority** (Article 77 GDPR). If a data subject considers the that the processing of personal data has infringed GDPR, the subject has the right to complain to the Office of the Information Commissioner (ICO). The procedure is set out on the ICO website.

The rights in relation to personal data set out under the GDPR are those of the individual to whom the data relates. The school will, in most cases, rely on parental or guardian consent to process data relating to pupils, and those with 'parental responsibility' are entitled to receive relevant information concerning the child. A pupil of sufficient maturity and understanding has certain legal rights which the school must observe. These include the right to give or withhold consent and certain rights to confidentiality. In exceptional circumstances, if a conflict of interest arises between a parent and a pupil, the rights of, and duties owed to the Pupil will in most cases take precedence over

[2] GDPR contains other rights of data subjects including objecting to automated decision making, profiling and the transfer of data outside of the EU. Such matters have not been included in this policy since Cransley School does not engage in them.

those of the parent.
Unless explicitly informed by parent or pupil, the school will continue to rely on parental or guardian consent in respect of processing pupils' data. See section on Rights of access by data subjects, page 15 of this Policy.* MUST CHECK THIS REFERENCE ONCE THE POLICY IS PUBLISHED ON THE WEBSITE SINCE FORMATTING WILL CHANGE THE PAGE NUMBER*

Restrictions of the rights of data subjects

The rights of data subjects are qualified by a number of restrictions listed in Article 23 of GDPR. In effect a data controller does not have to comply with the request of a data subject when a refusal is a necessary and proportionate measure to:

- safeguard national security, defence or public security;
- prevent or detect crime;
- safeguard other important objectives of public interest, for example, for the assessment of any tax or duty;
- ensure protection of legal proceedings,
- ensure the protection of the data subject and the rights and freedoms of others,
- ensure cooperation with regulatory authorities,

Security of personal data

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Cransley School and any third-party processor are required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This should include appropriate arrangements to ensure:

- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- the ongoing confidentiality, integrity, availability and resilience of processing systems

Accordingly, personal data will, so far as possible, be:

Kept in a locked filing cabinet; or

• In a locked drawer; or

• If it is computerised, be password protected; or

• Kept only on disk, or similar which itself is kept securely.

Data that fall within GDPR special categories will be subject to a further level of security where appropriate. For example, paper records will be kept within sealed envelopes inside locked drawers. Electronic records will be individually password protected and accessed only by means of password protected devices.

NOTE: Cransley School has an E-Safety Policy for ICT, Mobile devices and social networking. This policy should be adhered to at all times.
When personal data is to be destroyed, paper or microfilm records will be disposed of by shredding or incineration; computer hard disks or floppy disks will be reformatted, overwritten or degaussed.

All staff should be aware of the E-Safety Policy which is separate to this document and accessible via the Staff share server and the school website.

Personal data processed on behalf of Cransley School by third parties

Cransley School does transfer some personal data to third parties as part of its normal operations. One example is the payroll contractor who processes the information necessary for payment of salaries and deducting appropriate contributions for income tax, National Insurance etc.
The school only uses third parties who have provided sufficient guarantees that they implement appropriate technical and organisational measures to ensure the rights of data subjects. These measures are confirmed by means of contractual arrangements.

Personal data, unless otherwise exempt from restrictions on processing under the GDPR, will only be disclosed to third parties under the terms of this policy or otherwise with the consent of the appropriate individual.

Responsibilities under the GDPR

Cransley School, as a private company limited by guarantee, is the data controller under the GDPR.

The Board of Governors is responsible for the school's compliance with the GDPR and ensuring that other school policies and practices are consistent with this policy. The Board are responsible for ensuring that all staff are aware of their responsibilities under the act and appropriate training is put in place.

The Board of Governors have nominated one of their number to oversee compliance with this policy and associated procedures/instructions.

The Board of Governors have nominated a Data Compliance Manager with specific duties (Appendix A).

The Data Compliance Manager has appointed a Data Protection Co-ordinator with specific duties (Appendix A).

Notwithstanding the activities of nominated officers, compliance with the GDPR is the responsibility of all members of the school who process personal information.

Notification of personal data breaches

In the case of a personal data breach, the Data Compliance Manager will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the breach to the Office of the Information Commissioner (ICO) in accordance with Article 33 GDPR, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where a breach is a result of processing by a third party that third part must notify Cransley school's Data Compliance Manager without undue delay after becoming aware of it.

The notification referred to the ICO shall at least:

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.
b) communicate the name and contact details of the school's Data Compliance Manager or other contact point where more information can be obtained
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the school to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

(d) describe the measures taken or proposed to be taken by the school to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

When the personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Co-ordinator will communicate the personal data breach to the data subject without undue delay.

The communication to the data subject will describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of the previous paragraph.

Communication to data subjects is not be required if any of the following conditions are met

a) The school has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
b) The school has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to above are no longer likely to materialise.
c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner[3].

The Data Compliance Manager will maintain a record of data security incidents. This record will encompass both reportable and non-reportable incidents and be used as a resource of information to drive continual improvement.

Use of personal data by the school

The GDPR requires that the personal data held about pupils must only be used for specific purposes allowed by law. The school holds personal data on its pupils, including: contact details, assessment/examination results, attendance information, behaviour both positive and negative, and characteristics such as, special educational needs, any relevant medical information, and photographs.

The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care and to assess how well the school as a whole is doing, together with any other uses normally associated with this provision in an independent school environment.

[3] This provision of GDPR relates to breaches that affect many subjects and involve more than one data processor. This is unlikely to apply to Cransley School.

The school may make use of limited personal data (such as contact details) relating to pupils, their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school.

In particular, the school may:

a) Make available information to any internal association, society or club set up for the purpose of maintaining contact with pupils or for administration, fundraising, marketing or promotional purposes relating to the school, e.g. Alumni. The school will remain as data controller and this policy will govern data usage.

b) Make use of photographs of pupils in school publications and on the school's website. To this end parents/ guardians will be required to complete a Photography Consent form to indicate their wishes in respect of this matter. A blank form is attached at Appendix J.

c) Make personal data, including health–related personal data, available to staff for planning curricular or extra-curricular activities;

Parents who do not want their child's photograph or image to appear in any of the school's promotional material, or be otherwise published, must also make sure their child knows this.

Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use, the GDPR does not apply, e.g. where a parent takes a photograph of their child and some friends taking part in the school sports day. Parents or family members should seek permission to record events. Appendix K sets out the school's policy on this specific issue.

Occasionally the school may wish to post personal data relating to a pupil in relevant places so as to ensure the health and safety of that pupil. One example would be posting a photograph of a pupil with a severe nut-allergy. Such actions are permissible under GDPR however, the school will endeavour to ensure that parents/guardians are well aware of this practice and have given explicit consent.

Disclosure of personal data to third parties

The school may receive requests from third parties (i.e. those other than the data subject, the school, and employees of the school) to disclose personal data it holds about pupils, their parents or guardians. This information will not generally be disclosed unless:

- doing so is necessary for the legitimate interests of the individual concerned or the school, or
- the data subject has given explicit consent as part of the Privacy Notice completed when the personal data was collected (see Appendix D for the Privacy Notice format).

In any case, data subjects will be informed of the intention to disclose the relevant data at the time it is requested.

The following are the most usual reasons that the school may have for passing personal data to third parties. To:

a) give a confidential reference relating to a pupil;

b) give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend; please note that the school reserves the right to share personal information with third party credit reference agencies if it is considered by the school to be necessary.

c) publish the results of public examinations or other achievements of pupils of the school;

d) disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

e) provide information to another educational establishment to which a pupil is transferring;

f) provide information to the Examination Authority as part of the examinations process; and

g) provide the relevant information to the Government Department concerned with national education e.g. DfES.

The Department for Education uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them.

Data subjects have the right to withdraw consent at any time and to object to the processing of personal data pursuant to Article 18 GDPR. Any wish to make such a withdrawal or objection should be notified to the Data Protection Compliance Manager in writing.

Where the school receives a disclosure request from a third party it will take reasonable steps to verify the identity of that third party before making any disclosure. When members of staff receive enquiries from third parties for personal data, the enquirer should be asked why the information is required. If consent to the disclosure has not been given then the request should be declined. In normal circumstances information should not be disclosed over the phone to third parties. In most circumstances third parties should be asked to provide documentary evidence to support data requests.

Sharing data with third party organisations:

The school does not normally share data with third parties. Occasionally we facilitate the provision of personal, pastoral services to pupils on a 1:1 basis, for example the provision of counselling services. In such circumstances the school will seek to engage competent professionals and will confirm appropriate confidentiality and data security by means of a Service Level Agreement (SLA). See Appendices Q and R for the SLA templates that will be employed as appropriate.

Sharing data and safeguarding children:

The government publication "Working Together to Safeguard Children – July 2018" (updated 2019), is explicit in clarifying that the Data Protection Act 2018 and GDPR do not prohibit the collection and sharing of personal information to ensure effective safeguarding arrangements. Further, it states "*Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare, and protect the safety, of children, which must always be the paramount concern*".
Accordingly, when faced with safeguarding issues, Cransley School will share appropriate information with the relevant authorities, while ensuring the strictest confidentiality.
In such circumstances we will endeavour to obtain consent from parents and guardians, unless doing so would in itself lead to risk to a child, or the delay in doing so would lead to risk.
Further information on this subject can be found in the school's Safeguarding Policy.

Careers advice:

Pupils will be offered careers advice from independent contractors through an on-line service. In this situation, since the exchange of information is direct from pupil to careers advisor, Cransley School has no responsibilities under GDPR.
Accordingly, parents/guardians will be informed in advance and asked to confirm their consent to the service.

Cloud Computing:

Cransley School stores some personal data electronically on cloud services. The contractors that provide these services have been assessed by the school's IT advisors and selected only where they can provide such organisational and technical solutions that ensure that data is only stored on systems where it can be proven that of the rights of the data subjects are properly protected. These measures are formally confirmed by means of a written contract. The school's data protection staff and the school's IT advisors will take additional steps to visit and satisfy themselves that the measures described by the contractors are suitably effective.

At the time of drafting, the school is reviewing its position on cloud storage and use of social media. This section will be reviewed and revised as necessary once this process is complete.

Accuracy of personal data

The school will endeavour to ensure that all personal data held in relation to an individual is accurate. Individuals must notify the relevant school's Data Protection Coordinator in writing of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (see above).

The school will issue a confidential Data Check Sheet (Appendix H) to all parents/guardians on an annual basis to help with data accuracy.

Similarly, the school will issue a confidential Data Check Sheet (Appendix I) to all employees on an annual basis.

Rights of access by data subjects to their personal data

Under the GDPR, individuals have a right of access to their personal data held by the school. Accessing data is achieved by means of a Subject Access Request (SAR) (see below).

With regard to pupils, the ICO advise that a child may exercise all of the rights of data subjects on their own behalf as long as they are competent to do so. With regard to assessing the competence of individual children, the ICO states

"In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

What matters is whether the child is able to understand and deal with the implications of exercising their rights. So, for example, does the child understand what it means to request a copy of their data and how to interpret the

information they receive as a result of doing so? When considering borderline cases, you should take into account, among other things:

- *where possible, the child's level of maturity and their ability to make decisions like this;*
- *the nature of the personal data;*
- *any court orders relating to parental access or responsibility that may apply;*
- *any duty of confidence owed to the child or young person;*
- *any consequences of allowing those with parental responsibility access to exercise the child's rights. This is particularly important if there have been allegations of abuse or ill treatment;*
- *any detriment to the child or young person if individuals with parental responsibility cannot access this information; and*
- *any views the child or young person has on whether their parents should have access to information about them*".

Generally, in the case of pupils under the age of 12 years, the person with parental responsibility will exercise this right on their behalf. Pupils aged 12 years and over can exercise this right themselves or may authorise a parent, guardian or another to act on their behalf. The pupil's signature on the SAR form would be required in these circumstances.
Cransley School will, by default, consult with those with parental responsibility for individual pupils with respect to data protection matters unless instructed to do otherwise by pupils over the age of twelve or their parents/guardians. In such cases the above criteria will be applied.
In exceptional circumstances, if a conflict of interest arises between a parent and a pupil, the rights of, and duties owed to the pupil will in most cases take precedence over those of the parent.

Requests for access to records (Subject Access Requests)

A Subject Access Request (SAR) must be made in writing. The school may receive a request verbally or other form, therefore as soon as the request becomes manifest a Subject Access Request Form (Appendix B) must be sent to the applicant within two working days of when the initial request is received by the school.

All requests for access to records must be noted on the relevant pupil's file, and the Form forwarded from the Headmaster to the Data Compliance Manager via the school office. On receipt of the completed request form the school will:

• Record receipt and refer the request to the Data Compliance Manager.

• Forward the completed request to the Headteacher within 2 days of receipt.

The Data Compliance Manager will oversee and ensure that the SAR is completed as outlined in this policy.

An SAR will be accepted as long as satisfactory identification is given and the information request is clear, not excessive or vexatious. Where the pupil and parents are known to the school further identification will not be required. In other cases, photo identification such as a passport or driving licence will be required.

Responding to requests for access to records

The school will send a written response to the applicant acknowledging receipt of the application form. This must be done within 5 days of the request being received.

The school's Data Compliance Manager will manage the response to the applicant. The Data Compliance Manager will also maintain a SAR process sheet (Appendix O). The purpose of the process sheet is to identify and monitor deadlines and record contact with and information sent to the applicant. It will also record decisions taken with regard to the application.

The Headteacher must authorise the applicant's request for access before any information is disclosed.

The school may also wish to get advice from a Solicitor in relation to a disclosure.

If the applicant's request for access is granted, the information will be provided without delay and at the latest within one month of receipt. The GDPR allows data controllers to extend the period of compliance by a further two months where requests are complex or numerous. Where this is the case, the individual will be informed within one month of the receipt of the request and with an explanation the extension is necessary. However, in light of the nature of personal data held by the school, it is most unlikely that such an extension will be necessary.

Requests for access will not be granted until:

a) a written application is received by the Headmaster.

b) the school has received sufficient information to enable it to identify the individual who is seeking access; and

c) the school has received sufficient information to enable it to access the information requested.

Where an SAR is manifestly unfounded or excessive, the school is entitled to refuse the request or charge a reasonable fee for responding, particularly if it is repetitive. The fee will be based on the administrative cost of providing the information.
Otherwise, information provided in response to an SAR will be provided free of charge.

Once a request has been granted, the school will:

- Agree a secure method of releasing the records to the applicant.
- Where the conditions set out above are fulfilled, give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data are or may be disclosed.
- The school will also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information.

.

Exemptions to access by data subjects

Under S15 of the DPA 2018, data subjects are not entitled to information in respect of the following issues. In the event of an SAR referring to such matters, the school will inform the applicant that no information has been identified that is required to be supplied under GDPR and DPA.

Confidential references given, or to be given by the school are exempt from access. The school will therefore treat as exempt any reference given by them for the purpose of the education, training or employment, or prospective education, training or employment of any pupil or member of staff.

It should be noted that confidential references received from other parties may also be exempt from disclosure. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

Examination scripts, that is information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

Examination marks do not fall within an exemption as such. However, the one month compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the school received the request (if all the necessary conditions are fulfilled), or one month from the announcement of the examination results, whichever is the earlier.

An exemption may also be considered in cases where a third party is identified and disclosure may be detrimental to that party.

Data covered by Legal Privilege is also exempt i.e. where it may be necessary to take legal advice regarding a Data Subject; this information is exempt from Subject Access Request.

Collection of data

Personal data that falls into the scope of GDPR will be collected by Cransley School from, parents/guardians, employees and Friends of Cransley and Alumni. GDPR requires that at the time of collection data subjects are provided with the following information:

- the identity and the contact details of the controller;
- the contact details of the Data Compliance Manager, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- Where the processing is necessary for the purposes of the legitimate interests of the school, what those interests are;
- the recipients or categories of recipients of the personal data, if any;

There are also requirements relating to the transfer of data outside of the EU. The school will not do this without consultation and express consent from the data subject.

In addition, the school is required to provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request rectification or erasure of personal data or restriction of processing the data subject or to object to processing as well as the right to data portability;
- where the processing is based on the consent of the data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

Accordingly, each individual from whom data is collected will be required to complete a data consent form, generally known as a Privacy Notice, to ensure that explicit consent is obtained for the processing of that data that is necessary for the purposes of safeguarding and promoting the welfare of pupils, and where necessary, for the legitimate interests of the School and ensuring that all relevant legal obligations of the school and data subjects are complied with.

Privacy Notices for each of the above classes of individual are in Appendices D, E, F and G.

Where the school responds to a new enquirer, the letter that is sent out with a prospectus will contain the following text:

"*The personal data you supply to Cransley School will only be used in connection with your application for a school place. It will be held securely in line with the General Data Protection Regulation and will not be passed to third parties. Should you not join the school the data will be destroyed* in line with the school Data Protection Policy which is available on the school website".

Retention of data

The school will not keep pupil and related data for longer than necessary. Any records or part of records retained will be disposed of in line with the criteria set out in the Data Retention Schedule in Appendix L to this policy.
Brief details will be retained on all pupils indefinitely for Alumni and PR purposes. These details will include: name of pupil, date of birth, address, telephone number, email address, name of parents, gender of pupil, year pupil joined the school, previous school, new school, joining date, leaving date, parents' occupations, year group on leaving.

Exceptions to the above include records where there may be ongoing litigation in which case the entire record will be retained until final disposition of the matter and thereafter for a period of 7 years.

Further, at the time of drafting this Policy an official Independent Inquiry into Child Sexual Abuse is underway. An instruction has been issued that all files that may have safeguarding implications are retained indefinitely, or at least until the conclusion of the Inquiry. Cransley School will comply with this instruction.

A Disposal Log (Appendix M) will be maintained to list which records have been deleted, the date and description.

Personal details of pupil applicants which did not progress from Junior to Senior school will be disposed of after 2 years.

Staff records will be securely disposed of 7 years after a member of staff leaves Cransley School's employment. Brief details will be retained on all staff indefinitely to satisfy future reference requests. These details will include full name, date of birth, job title, national insurance number and period of employment.
Exceptions to this include records where there may be ongoing litigation in which case the entire record will be retained until final disposition of the matter and thereafter for a period of 7 years.

Unsuccessful staff applications will be kept for 6 months after interview.

Accident books / logs relating to all accidents in school will be kept for 40 years after the accident has been recorded as a claim relating to certain exposures or injuries could be made up to that time. The accident book will meet HSE accident and injury reporting requirements[4],[5].

A flagging process will also be maintained to identify those records which should not be deleted due to litigation or other reasons. The flagging process and accident log will be referred to prior to records being deleted to identify any exceptions.

Disposal of data

Please see Appendix L, Data Retention Guide.

Audit

An audit of the school's compliance with this policy will be carried out on an annual basis by the Data Protection Coordinator in conjunction with the nominated Governor with responsibility for data protection. This audit will be coordinated by the Data Compliance Manager(See Appendix C).

The Annual Data Protection Audit Return will report using the form in Appendix T.

The S.A.R. process will also be tested annually by the Data Compliance Manager . This will be done by choosing a data subject at random and completing a S.A.R process sheet within the specified time detailing all the information gathered for that subject. In line with the policy the process sheet will be forwarded to the Data Compliance Manager and the nominated Governor for feedback and action.

Publishing examination results:

Publishing examination results is a common and accepted practice. The GDPR does not stop this happening since doing so is in the legitimate interests of the school. However, GDPR expects the school to act fairly when publishing results and where people have concerns about their or their child's information being published, schools must take those concerns seriously.

Objections

Since the school has a legitimate interest in publishing examination results, pupils or their parents or guardians do not need to give their consent to publication. However, parents and guardians do have the opportunity to opt out of identifying individuals on an annual basis when they are asked to review their personal data.

Staff Data

Staff are made aware of, and agree to their data being processed by Cransley School by completing and signing their Privacy Notices.

Special categories of personal data will only be used by Cransley School for legitimate business, management and school purposes and will not be transferred to third parties without consent.

Staff data will be held securely in locked cabinets or password protected electronic formats.

[4] An Accident is any unplanned or undesired event that results in injury to a person which requires significant first aid intervention.

[5] Accident and injury reporting is governed by the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013

Access to staff records will be limited to those personnel appointed by the Headteacher as appropriate for specific purposes.

As with all data subjects, staff may request to see, or have a copy of their record under the Subject Access Request provision of the GDPR. The process is described above and a copy of an SAR form can be found in Appendix B Subject Access Requests should be made to the Headteacher.

Staff records will normally be kept for 7 years after their employment has ceased. Unsuccessful applicants will have their data kept for 6 months after their application. See the Data Retention Guide in AppendixL

The Data Protection Co-ordinator will address the retention periods in the annual audit. The Data Protection Co-ordinator will also oversee the secure disposal of expired data.

DBS checks are carried out routinely by Cransley School Staff. Records will only indicate whether a satisfactory or unsatisfactory check has been received. No additional details regarding the DBS check will be held on the staff record.

CRANSLEY SCHOOL

Appendix A : Roles and Responsibilities

Data Compliance Manager

The role of the Data Compliance Manager (DCM) is to:

• Ensure that the organisation complies with the GDPR, and to ensure that employees are fully informed of their own responsibilities for acting within the law and that data subjects, including employees, are informed of their rights under the Regulation.

• Be the point of contact with the Office of the Information Commissioner (ICO), notify any breaches of security and cooperate with the ICO on other matters relating to processing.

• Oversee GDPR activities (including training) and facilitate such user group meetings as necessary e.g. The General Purpose Committee.

• Oversee the activities of the Data Protection Coordinator to ensure compliance with this policy.

• Ensure organisational compliance, and conformance with data protection principles

• Develop, implement and enforce a suitable and relevant Data Protection Policy and ensure it is reviewed on an annual basis

• To oversee systematic GDPR compliance audits.

• Manage investigations into complaints about breaches of GDPR and undertake reporting/remedial action as required. Maintain a log of any incidents and remedial recommendations and actions.

- Act as a focal point coordinating the activities of the school's Governors and IT Advisors in respect of GDPR matters.

• Maintain a log of and co-ordinate Subject Access Requests.

• Maintain and update own knowledge of developments in data protection issues.

• Be a resource for other employees by providing expert advice on GDPR and related issues.

Role of the Headteacher

The Headteacher is responsible for the successful implementation of this policy in their school. The Headteacher will agree and authorise all data to be released in connection with a Subject Access Request.

Data Protection Coordinator

The role of the Data Protection Coordinator is to:

• Act as first point of contact for internal data protection enquiries.

- Co-ordinate compliance with the GDPR across Cransley School and will be supported by the Data Compliance Manager with the following:

o On Site Data Security.

o Compliance Audit.

- Training.
- Subject Access Requests.
- Supplementing, review and update of policy and procedures.
- Housekeeping/compliance e.g. data archiving, deletion etc.
- Maintain and update own knowledge of developments in data protection issues.

CRANSLEY SCHOOL

Appendix B : Subject Access Request Form

Request for information under the General Data Protection Regulation 2018

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type.

1. Personal details of the person requesting the information.

Surname:	
Forename:	
Address:	
Postcode:	
Telephone number:	
Email:	

2. Are you the Data Subject (i.e. the person whose information you are requesting)?

Please tick the appropriate box.

Yes □ (Please go straight to question 5)

No □

3. Personal details of the Data Subject (if different from those at section 1).

Surname:	
Forename:	
Address:	
Postcode:	
Date of birth	
Telephone number:	
Email:	

4. Please describe your relationship with the Data Subject that leads you to make this request on their behalf.

---

5. Information requested

Please describe below the information or only specific document(s) you wish to see, ----------

---

Declaration

I certify that the information given in this application form to the school is true. I understand that it will be necessary for the school to confirm my/the data subject's identity and it may be necessary to supply more detailed information if required.

I have read and understood the school's Data Protection Policy and confirm that this request accords with that policy.
I understand that I am not entitled to access to the personal data of other persons and that, if necessary, information supplied in response to this request may be edited or redacted accordingly.

Signature
(Parental Responsibility/employee*) ----------

Print name ----------

Date: ----------

Signature
(Pupil 12 +*) ----------

General Data Protection Regulation 2018

The Data Controller is Cransley School Ltd.

The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

The Headmaster,
Cransley School, Belmont Hall, Great Budworth, Cheshire, CW9 6H

The school will send a written response acknowledging receipt of this application form within 5 days of receipt. If the request for access is granted, the information will be provided without delay and at the latest within one month of receipt. The GDPR allows data controllers to extend the period of compliance by a further two months where requests are complex or numerous. In the unlikely event of this being the case, applicants will be informed within one month of the receipt of the request and with an explanation the extension is necessary. Applicants should be aware that under certain circumstances the school is entitled to decline a Subject Access Request and are urged to refer to the school's Data Protection Policy which can be found on the school website (https://cransleyschool.com/documents-and-policies).

Office use only

Received by:	Date:
Forwarded to:	Date:
Date to be completed by:	
Comments:	

CRANSLEY SCHOOL

Appendix C : Audit Outline

1. Aims of Data Protection Compliance Audits

• to ensure that information is obtained and processed fairly, lawfully and on a proper basis.

• Quality Assurance, ensures that information is accurate, complete and up-to-date, adequate, relevant and not excessive.

• Retention processes ensure appropriate weeding and deletion of information.

• Authorised use of systems is documented, e.g. data security policy, guidance, procedures.

• Mechanisms exist to ensure compliance with individual's rights, such as subject access.

• To assess the level of compliance with the organisation's own data protection system.

• To identify potential gaps and weaknesses in the data protection system.

• To provide information for data protection system review.

2. Audit Objectives

When carrying out a Data Protection Audit, the auditor has three clear objectives:

I. To verify that there is a formal (i.e. documented and up-to-date) data protection system in place in the area.

II. To verify that all the staff in the area involved in data protection:

a. Are aware of the existence of the data protection system;
b. Understand the data protection system;
c. Use the data protection system.

III. To verify that the data protection system in the area actually works and is effective.

3. Areas to be examined include:

• Use of appropriate forms when collecting data.

• Storage of data in accordance with the security policy, e.g. locked cabinets, passwords, etc.

• Data being removed in accordance with policy timescales.

• Subject Access Request process in place.

• Staff training requirements assessed and highlighted.

CRANSLEY SCHOOL

Appendix D : Privacy Notice(Parent/pupil)[6]

Cransley School Ltd is a Data Controller as defined by the General Data Protection Regulation 2018 (GDPR) and as such has duties to use information or personal data it collects from individuals as part of its legitimate business activities, in ways that protect the fundamental rights and freedoms of the individuals providing that information. GDPR applies to "*personal data*" which is defined as "*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as a name, identification number, location data or similar*".
The purpose of this Notice is to explain: what information we collect about you; how we will use it; you rights in respect to how we keep and use your information, how to access information we hold about you; and to obtain your consent to us processing[7] your information. More detailed information on the following issues can be found in the school's Data Protection Policy that can be found on the school website at https://cransleyschool.com/documents-and-policies

The information we collect about you:

When you join the school, we collect information about parents/guardians and about pupils via a registration form. The information includes basic details to identify parents and pupils and to allow us to communicate effectively with you. More confidential information is collected concerning the health of pupils and where relevant their previous education experience, to enable us to care for them effectively in the school environment, to ensure their safety and to aid their development throughout their school life.
Further information is collected from parents/guardians to inform the payment of fees and similar.
Throughout their time at school additional data is generated about pupils that falls within the scope of the GDPR, for example, examination results.

How we will use the information we hold:

This information will be used to inform the normal business of running a school such as; organising and conducting classes, communicating with parents /guardians, administering fees and payments, organising external educational activities and promoting the school and the achievements of pupils. In doing so we will:

- only use personal data in ways that are lawful, fair and in a transparent manner,
- only hold such data as is adequate, relevant and limited to what is necessary to carry out the legitimate activities of the school and safeguard pupils,
- ensure that data is accurate and up to date. To this end we will issue confidential data collection check sheets annually.
- keep data no longer than is necessary. Our Data Retention Guide is appended to of the school's Data Protection Policy that can be found on the school website.
- employ suitable and effective systems that ensure that personal data including sensitive information is kept secure against unauthorised access, loss, destruction or damage.

Your rights under GDPR:

Data subjects have the following rights:

- The right of **access** to the data to; confirm its nature and how it is used, how long it will be stored and obtain a copy.
- The right to **rectification**; to correct inaccurate data, and to have incomplete data completed.
- The right to have data e**rasure** where it is no longer necessary for it to be kept, if you no longer consent or object to it being kept, or it has to be erased to comply with a legal obligation.
- The right to the **restriction of processing** where; the accuracy of the data is contested or you object to it being used.
- The right to **object** to us using your data.

[6] All Privacy Notices in this Policy have been checked and found to comply with the ICO Code of practice on communicating privacy information to individuals. {https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf}
[7] "Processing" is the term used by GDPR to describe what is done to/with data. Here it refers to Cransley School storing and using data in the ways described in this notice.

The right to **lodge a complaint with the Office of the Information Commissioner (ICO)**. The procedure is set out on the ICO website.

You have other rights relating to the use of personal data but these are very unlikely to affect the way Cransley School uses your data. For full details you can read the school's Data Protection Policy on https://cransleyschool.com/documents-and-policies or go direct to the ICO website.

Access to your information:

To ensure the security of your information, prevent unauthorised access and accuracy of response, the school operates a Subject Access Request system. Should you wish to access the information the school holds on you or your child, in whole or part, please complete a Subject Access Request form. This can be found in Appendix B of the school's Data Protection Policy that can be found on the school website.

Sharing your information:

The school will not under normal circumstances share your information with any other person or organisation without your knowledge or consent. Examples where we would seek to share information are the provision of careers advice or engaging counselling services. However, in exceptional circumstances we may share information with responsible agencies; for example, where the vital interests of a child are concerned (safety or health -related), or where we are legally obliged to do so.
In instances of dispute, financial or otherwise we may share information with our legal advisors.

Consent:

GDPR requires that Data Controllers such as Cransley School Ltd obtain consent from individuals who provide them with data in order to lawfully make use of that data. **If you consent to the school using the information you have supplied in the pupil information forms and the confidential data collection check sheets in the manner described above, please tick the following box:**

☐ I agree to Cransley School processing the data I have provided within the terms of this Privacy Notice and the school's Data Protection Policy.

Communications:

The school will want to and may well need to contact you regularly with information relating to school schedules, holidays, events and similar. **Please tick the boxes below to indicate your consent to us contacting you via the means listed.**

☐ Post ☐ Phone ☐ Email ☐ Text/SMS ☐ Automated phone call

I understand that I may withdraw consent to all or any of the above items at any time. To do so or to obtain information on Cransley School's data protection activities I must contact Mr N Willets Deputy Head, Cransley School.

Signature
(Parent/guardian) ----------

Print name ----------

Date: ----------

Appendix E : Privacy Notice (Employee)

Cransley School Ltd is a Data Controller as defined by the General Data Protection Regulation 2018 (GDPR) and as such has duties to use information or personal data it collects from individuals as part of its legitimate business activities in ways that protect the fundamental rights and freedoms of the individuals providing that information. GDPR applies to "*personal data*" which is defined as "*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as a name, identification number, location data or similar*".
The purpose of this Notice is to explain: what information we collect about you; how we will use it; you rights in respect to how we keep and use your information, how to access information we hold about you; and to obtain your consent to us processing[8] your information. More detailed information on the following issues can be found in the school's Data Protection Policy that can be found on the school website at https://cransleyschool.com/documents-and-policies

The information we collect about you:

When you join the school, we collect information about you mainly via your application form and a new-starter payroll details form. Further, more confidential information is collected via other paperwork. This information enables us to manage the school effectively, pay you and to allow us to meet our legal duties, e.g. safeguarding children, tax & employment law, health & safety at work. Throughout your time at school additional data is generated about you that falls within the scope of the GDPR, for example, work appraisals and even photographs taken[9].

How we will use the information we hold:

This information will be used to inform the normal business of running a school. In doing so we will:

- only use personal data in ways that are lawful, fair and in a transparent manner,
- only hold such data as is adequate, relevant and limited to what is necessary to carry out the legitimate activities of the school and safeguard pupils,
- ensure that data is accurate and up to date. To this end we will issue confidential data collection check sheets annually.
- keep data no longer than is necessary. Our Data Retention Guide is appended to of the school's Data Protection Policy that can be found on the school website.
- employ suitable and effective systems that ensure that personal data including sensitive information is kept secure against unauthorised access, loss, destruction or damage.

Your rights under GDPR:

Data subjects have the following rights:

- The right of **access** to the data to; confirm its nature and how it is used, how long it will be stored and obtain a copy.
- The right to **rectification**; to correct inaccurate data, and to have incomplete data completed.
- The right to have data e**rasure** where it is no longer necessary for it to be kept, if you no longer consent or object to it being kept, or it has to be erased to comply with a legal obligation.
- The right to the **restriction of processing** where; the accuracy of the data is contested or you object to it being used.
- The right to **object** to us using your data.
- The right to **lodge a complaint with the Office of the Information Commissioner (ICO)**. The procedure is set out on the ICO website.

You have other rights relating to the use of personal data but these are very unlikely to affect the way Cransley School uses your data. For full details you can read the school's Data Protection Policy on https://cransleyschool.com/documents-and-policies or go direct to the ICO website.

[8] "Processing" is the term used by GDPR to describe what is done to/with data. Here it refers to Cransley School storing and using data in the ways described in this notice.
[9] Photographs and similar are subject to a separate consent form that can be found at Appendix I of the school's Data Protection Policy.

Access to your information:

To ensure the security of your information, prevent unauthorised access and accuracy of response, the school operates a Subject Access Request system. Should you wish to access the information the school holds on you or your child, in whole or part, please complete a Subject Access Request form. This can be found in Appendix B of the school's Data Protection Policy that can be found on the school website.

Sharing your information:

The school will not under normal circumstances share your information with any other person or organisation without your knowledge or consent. Examples where we would seek to share information are using a payroll contractor to assist in paying salaries and using the services of a pensions advisor in administering the school's pension scheme. However, in exceptional circumstances we may share information with responsible agencies where we are legally obliged to do so e.g. HMRC.
In instances of dispute, financial or otherwise we may share information with our legal advisors.

Consent:

GDPR requires that Data Controllers such as Cransley School Ltd obtain consent from individuals who provide them with data in order to lawfully make use of that data. **If you consent to the school using the information you have supplied as described above, please tick the following box:**

☐ I agree to Cransley School processing the data I have provided within the terms of this Privacy Notice and the school's Data Protection Policy.

Communications:

The school will normally communicate with you via briefings and your school email account. However, not all staff have school email accounts. On occasion, we may need to contact you using your personal means. **Please tick the boxes below to indicate your consent to us contacting you via the means listed.**

☐ Post ☐ Phone ☐ Email ☐ Text/SMS ☐ Automated phone call

Data sharing:

☐ **I agree to Cransley School sharing information with the school's payroll contractor and Pensions Advisor.**

I understand that I may withdraw consent to all or any of the above items at any time. To do so or to obtain further information on Cransley School's data protection activities I must contact Mr N Willets Deputy Head, Cransley School.

Signature ----------

Print name ----------

Date: ----------

Appendix F : Privacy Notice(Alumni)

Cransley School Ltd is a Data Controller as defined by the General Data Protection Regulation 2018 (GDPR) and as such has duties to collect and use information or personal data it collects from individuals as part of its legitimate business activities in ways that protect the fundamental rights and freedoms of the individuals providing that information. GDPR applies to "*personal data*" which is defined as "*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as a name, identification number, location data or similar*".
The purpose of this Notice is to explain: what information we collect about you; how we will use it; you rights in respect to how we keep and use your information, how to access information we hold about you; and to obtain your consent to us processing[10] your information. More detailed information on the following issues can be found in the school's Data Protection Policy that can be found on the school website at https://cransleyschool.com/documents-and-policies.

The information we collect about you:

When you left the school, we retained some information about you which was necessary for us to meet our legal duties. In addition, we have kept basic information such as names, addresses and contact details so that we can stay in contact with you to share our news, receive news from you and let you know about special events and similar.

How we will use the information we hold:

We will:

- only use your personal data in ways that are lawful, fair and in a transparent manner,
- only hold such data as is adequate, relevant and limited to what is necessary to carry out the legitimate activities of the school,
- ensure that data is accurate and up to date. To this end we request you inform us of any changes so that we can communicate with you efficiently.
- keep data no longer than is necessary. Our Data Retention Guide is appended to of the school's Data Protection Policy that can be found on the school website.
- employ suitable and effective systems that ensure that personal data including sensitive information is kept secure against unauthorised access, loss, destruction or damage.

Your rights under GDPR:

Data subjects have the following rights:

- The right of **access** to the data to; confirm its nature and how it is used, how long it will be stored and obtain a copy.
- The right to **rectification**; to correct inaccurate data, and to have incomplete data completed.
- The right to have data e**rasure** where it is no longer necessary for it to be kept, if you no longer consent or object to it being kept, or it has to be erased to comply with a legal obligation.
- The right to the **restriction of processing** where; the accuracy of the data is contested or you object to it being used.
- The right to **object** to us using your data.
- The right to **lodge a complaint with the Office of the Information Commissioner (ICO)**. The procedure is set out on the ICO website.

You have other rights relating to the use of personal data but these are very unlikely to affect the way Cransley School uses your data. For full details you can read the school's Data Protection Policy on https://cransleyschool.com/documents-and-policies or go direct to the ICO website.

[10] "Processing" is the term used by GDPR to describe what is done to/with data. Here it refers to Cransley School storing and using data in the ways described in this notice.

Access to your information:

To ensure the security of your information, prevent unauthorised access and accuracy of response, the school operates a Subject Access Request system. Should you wish to access the information the school holds on you or your child, in whole or part, please complete a Subject Access Request form. This can be found in Appendix B of the school's Data Protection Policy that can be found on the school website.

Sharing your information:

The school will not under normal circumstances share your information with any other person or organisation without your knowledge or consent. However, in exceptional circumstances we may share information where we are legally obliged to do so.

Consent:

GDPR requires that Data Controllers such as Cransley School Ltd obtain consent from individuals who provide them with data in order to lawfully make use of that data. **If you consent to the school using the information you have supplied in the manner described above, please tick the following box:**

☐ I agree to Cransley School processing the data I have provided within the terms of this Privacy Notice and the school's Data Protection Policy.

Communications:

The school will want to contact you with information relating to school events and similar. **Please tick the boxes below to indicate your consent to us contacting you via the means listed.**

☐ Post ☐ Phone ☐ Email ☐ Text/SMS ☐ Automated phone call

I understand that I may withdraw consent to all or any of the above items at any time. To do so or to obtain information on Cransley School's data protection activities I must contact Mr N Willets Deputy Head, Cransley School.

Signature ----------

Print name ----------

Date: ----------

Appendix G : Privacy Notice(Governors & Friends of Cransley)

Cransley School Ltd is a Data Controller as defined by the General Data Protection Regulation 2018 (GDPR) and as such has duties to use information or personal data it collects from individuals as part of its legitimate business activities in ways that protect the fundamental rights and freedoms of the individuals providing that information. GDPR applies to "*personal data*" which is defined as "*any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier such as a name, identification number, location data or similar*".
The purpose of this Notice is to explain: what information we collect about you; how we will use it; you rights in respect to how we keep and use your information, how to access information we hold about you; and to obtain your consent to us processing[11] your information. More detailed information on the following issues can be found in the school's Data Protection Policy that can be found on the school website at https://cransleyschool.com/documents-and-policies

The information we collect about you:

When you join the school, we collect information about you that enables us to manage the school effectively and to allow us to meet our legal duties, e.g. safeguarding children. Throughout your time with the school additional data may generated about you that falls within the scope of the GDPR, for example, photographs taken to publicise achievements and events[12].

How we will use the information we hold:

This information will be used to inform the normal business of running a school. In doing so we will:

- only use personal data in ways that are lawful, fair and in a transparent manner,
- only hold such data as is adequate, relevant and limited to what is necessary to carry out the legitimate activities of the school and safeguard pupils,
- ensure that data is accurate and up to date. To this end we will issue confidential data collection check sheets annually.
- keep data no longer than is necessary. Our Data Retention Guide is appended to of the school's Data Protection Policy that can be found on the school website.
- employ suitable and effective systems that ensure that personal data including sensitive information is kept secure against unauthorised access, loss, destruction or damage.

Your rights under GDPR:

Data subjects have the following rights:

- The right of **access** to the data to; confirm its nature and how it is used, how long it will be stored and obtain a copy.
- The right to **rectification**; to correct inaccurate data, and to have incomplete data completed.
- The right to have data e**rasure** where it is no longer necessary for it to be kept, if you no longer consent or object to it being kept, or it has to be erased to comply with a legal obligation.
- The right to the **restriction of processing** where; the accuracy of the data is contested or you object to it being used.
- The right to **object** to us using your data.
- The right to **lodge a complaint with the Office of the Information Commissioner (ICO)**. The procedure is set out on the ICO website.

You have other rights relating to the use of personal data but these are very unlikely to affect the way Cransley School uses your data. For full details you can read the school's Data Protection Policy on https://cransleyschool.com/documents-and-policies or go direct to the ICO website.

[11] "Processing" is the term used by GDPR to describe what is done to/with data. Here it refers to Cransley School storing and using data in the ways described in this notice.
[12] Photographs and similar are subject to a separate consent form that can be found at Appendix I of the school's Data Protection Policy.

Access to your information:

To ensure the security of your information, prevent unauthorised access and accuracy of response, the school operates a Subject Access Request system. Should you wish to access the information the school holds on you, in whole or part, please complete a Subject Access Request form. This can be found in Appendix B of the school's Data Protection Policy that can be found on the school website.

Sharing your information:

The school will not under normal circumstances share your information with any other person or organisation without your knowledge or consent. However, in exceptional circumstances we may share information where we are legally obliged to do so.

Consent:

GDPR requires that Data Controllers such as Cransley School Ltd obtain consent from individuals who provide them with data in order to lawfully make use of that data. **If you consent to the school using the information you have supplied as described above, please tick the following box:**

☐ I agree to Cransley School processing the data I have provided within the terms of this Privacy Notice and the school's Data Protection Policy.

Communications:

The school will normally communicate with you via email. On occasion, we may need to contact you using your personal means. **Please tick the boxes below to indicate your consent to us contacting you via the means listed.**

☐ Post ☐ Phone ☐ Email ☐ Text/SMS ☐ Automated phone call

I understand that I may withdraw consent to all or any of the above items at any time. To do so or to obtain further information on Cransley School's data protection activities I must contact Mr N Willets Deputy Head, Cransley School.

Signature ----------

Print name ----------

Date: ----------

CRANSLEY SCHOOL

Appendix H : Data Collection Check Sheet(Parent/pupil)

As set out in the Privacy Notice you previously signed, Cransley School has a legal duty to ensure that personal data kept by the school is accurate and up to date**. Please check that the information below is correct. Complete any missing details and return to the school office IN A SEALED ENVELOPE to ensure confidentiality.**

Surname			**Legal Surname**		
Forename			**Middle name**		
Chosen name			**Gender**		
Date of Birth		**Year**		**Reg Group**	
Address					
Post Code					
Telephone					
Email					

Please give details of all persons who have parental responsibility and anyone else you wish to be contacted in an emergency. Place them in the order that you wish for them to be contacted in an emergency.

Priority	**Name/Relationship**	**Home Address /Phone /Mobile /Fax**	**Work Address Phone/Email**
1			
2			
3			

Pupil's dietary needs	

Medical Practice: Address:	
Telephone Number:	
Medical Practice: Address:	

Medical Condition(s)	

Medical Note(s):	

Ethnicity Religion:			
Home Language		**Religion**	
I confirm the above details are correct;			
Signature:		**Date:**	

CRANSLEY SCHOOL

Appendix I : Data Collection Check Sheet(Employee)

As set out in the Privacy Notice you previously signed, Cransley School has a legal duty to ensure that personal data kept by the school is accurate and up to date**. We hold the following basic information supplied by you. Please check that it is correct. Complete any missing details and return to the school office IN A SEALED ENVELOPE to ensure confidentiality.**

Surname			**Legal Surname**		
Forename			**Middle name**		
Chosen name			**Gender**		
Date of Birth					
Address					
Post Code					
Telephone					
Email					

The school's Finance Department also holds confidential information from you in order to pay your salary, contribute to the school pension scheme and to comply with HMRC requirements. Any changes in this information over the last 12 months must be conveyed directly to the Finance Department without delay.

CRANSLEY SCHOOL

Appendix J : Photography Consent Form

PHOTOGRAPH /VIDEO/ ARTWORK CONSENT AND RELEASE.

We would like to take photographs and videos of the pupils and parents to use on the school's promotional material such as the prospectus, website and editorial. We may wish to use photographs or videos of the children for other purposes such as class projects. Is it not practical to list every possible use but the following list gives some examples:

- Website
- Social media
- Prospectus
- Editorial
- Newspaper articles
- School directories
- Class projects

Please complete and sign the form below and return to the school.

Photographs of pupils:

I consent/do not consent (delete as appropriate) for my child's photograph or video image to appear in promotional and other material for the school**. Parents who do not want their child's photograph or image to appear in any of the school's promotional material, or be otherwise published, must also make sure their child knows this.**

Occasionally we may wish to publish a name with a photograph or video image. **Please tick here to indicate your consent to publishing your child's name with a photograph or video.** ☐

Name of child: _____

Name of parent/guardian: _____

Signature of parent/guardian: _____

Address: _____Date:_____

Photographs of parents/guardians

I consent/do not consent (delete as appropriate) to our photograph or video image to appear in promotional and other material for the school.

Occasionally we may wish to publish a name with a photograph or video image. **Please tick here to indicate your consent to publishing your name with a photograph or video.** ☐

Name of parent/guardian: _____

Signature of parent/guardian: _____

Please note you may alter this consent by contacting the school at any point.

CRANSLEY SCHOOL

Appendix K : Parents wishing to use photography and/or video a school event

Generally, photographs and videos for school and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves.
While this issue is not subject to data protection laws, Cransley School recognises that parents and guardians will have firm views on recording images of their children. The school has therefore adopted the following guidelines and expects that parents will willing comply with them.

- Remember that parents/carers and others, attend school events at the invitation of the Headteacher.
- The Headteacher has the responsibility to decide if photography and videoing of school performances is permitted.
- The Headteacher has the responsibility to decide the conditions that will apply so that children are kept safe and that the performance is not disrupted and children and staff not distracted.
- Parents and carers can use photographs and videos taken at a school event for their own personal use only. Such photos and videos must not be sold and must not be put on the public facing social media networks.
  Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.
- Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.
- Parents and carers must not photograph or video children changing for performances or events.
- If you are accompanied or represented by people that school staff do not recognise they may need to check who they are if they are using a camera or video recorder.
- Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.
- In exceptional circumstances e.g. child protection orders, the parent and Headteacher may agree an alternative and practical approach to this policy for specific pupils.

CRANSLEY SCHOOL

Appendix L: Data Retention Guide

1. Purpose of the Data Retention Guide

In the course of its activities every school creates and receives a large amount of information. Much of this information contains personal data the use of which is subject to the GDPR.

Personal data is any information relating to a living individual and would include information on pupils, members of staff and other employees. Data is very widely construed and can include internal files, letters, faxes, memoranda and notes, email, computer data and even voicemail and SMS images created or received in the course of operations.
GDPR distinguishes s**pecial categories of personal data** which are information in respect of; racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or orientation. This also includes; genetic data and biometric data where processed to uniquely identify an individual. Special categories of personal data can only be processed[13] under strict conditions.
Personal data referring to criminal convictions and alleged offences are not classed as special categories of personal data by the GDPR, but similar safeguards apply to its processing.

It is extremely important that data is held for the correct period of time so as to be available for the proper needs of the school. Indeed, some classes of data are required by law or good business practice to be kept for a specified period of time and failure to do so may at best prejudice the position of Cransley School and at worst expose the group or its staff and employees to potential lawsuits and/or fines or even put them in contempt of court. However, keeping all data for an unlimited period of time will not only be impractical but will also expose Cransley School to risk under the GDPR. This is because the retention of unnecessary data will create a compliance risk since the GDPR requires that personal data is:

- Adequate relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary

The excessive storage of data is not only highly obstructive to the smooth operation of the school but will also create a risk of prejudicing some or all of the above data protection principles.

The purpose of this guide is to provide guidelines for the retention, storage and disposal of the data held by the school. It applies across the school to all data received and held whatever format that data is held in.

2. Methods of retaining/storing personal data

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Accordingly, personal data will, so far as possible, be:

Kept in a locked room or cabinet; or

- In a locked drawer; or

- If it is computerised, be password protected; or

[13] Processing under GDPR includes storing and retaining data.

• Kept only on disk, or similar which itself is kept securely.

Data that fall within GDPR special categories will be subject to a further level of security where appropriate. For example, paper records will be kept within sealed envelopes inside locked drawers.

3. Retention Periods

Except as otherwise indicated in accordance with paragraph 5 below data should be retained for the number of years indicated in the Retention Schedule below.

Where, in accordance with paragraph 5, it is necessary for the school to retain certain data for a period beyond the period indicated in the schedule, the school will maintain a flagging process to identify those records which must be retained beyond the specified period. Unless a flag has been given in respect of specific data then data should be destroyed as soon as practicable after expiry of the specified retention period.

4. Disposal of Data

A document which is to be destroyed in accordance with this guide is likely still to be sensitive in the wrong hands, to deal with confidential or personal matters and/or have other security implications. The method by which these types of documents are disposed is of importance both because of the inherent risk such material falling into the wrong hands and because in accordance with the GDPR, Cransley School has a legal duty to ensure that it is disposed of securely. The method of disposal of data shall be consistent with the type of data being destroyed. Confidential data should be disposed of in a way that prevents the data from being accessible to others.

The main disposal methods and safeguards are as follows:

• Shredding.

- For individual documents cross-cutting shredder will be used,
- For bulk e.g. the annual disposal of documentation no longer required, an approved contractor will be used and certified confirmation of secure disposal will be obtained.

• Incineration. Consideration will be given to incineration of storage media where other methods of destruction are not deemed adequate.

• Overwriting electronic data, or otherwise making it unreadable. Care will be taken to ensure that sensitive data is completely erased. For example, deleting a file on a PC may only delete the file reference and not the underlying data. Extra care will also be taken to ensure the secure disposal of physical IT equipment upon which the personal data may have been held or processed.

5. Archiving data

In general, once data or documents are no longer "live" they will be moved to archiving as soon as is reasonably possible. NOTE: archived data and documents carry with them on-going obligations and are subject to the requirements of GDPR, for instance, archived data and documents will need to be considered in the event of any Subject Access Request and the archiving system will be kept properly secure.

Data and documents which have been archived will be reviewed against the criteria set out in this guide with a view to destruction after the relevant time period.

6. Retention of Data beyond the Retention Period

Where data should be retained indefinitely:

(1) If the school receives notice of any lawsuit, government or regulatory investigation (for instance, health & safety investigations), other legal action, complaint or claim against or involving:

a. Cransley School Ltd,
b. the school or any member of staff, or employee,
c. a pupil, or
d. any of circumstances likely to give rise to such an action, proceeding, investigation complaint or claim,

all data which may be relevant must be preserved and shall not be destroyed.

(2) If any member of staff or employee becomes aware that any notice has been received by the school of any lawsuit, government or regulatory investigation, other legal action, complaint or claim against or involving Cransley School Ltd or any member of staff, employee or pupil or any of circumstances likely to give rise to such an action, proceeding, investigation, complaint or claim, that member of staff or employee should immediately notify the school's Data Protection Co-ordinator in order that the Co-ordinator can review which data should be flagged for extended retention in accordance with this guide.
The member of staff or employee must not destroy any data relevant to such action, proceeding, investigation, complaint or claim whether it not it would otherwise fall to be destroyed in accordance with this guide.

(3) If any member of staff or employee is unsure whether any unflagged data is relevant to an action, proceeding, investigation complaint or claim the member of staff or employee should not delete that data and should liaise with the Data Protection Coordinator.

Once data has been flagged, all members of staff and employees must preserve and prevent the destruction of any such data (including e-mails and other computer records).

Destruction of such data, even if inadvertent, could seriously prejudice the member of staff, employee, or the school and could subject the individual or the school to substantial criminal and civil liability including fines and other penalties.

Whenever data is flagged the data must be preserved until the flag is removed. The communication imposing the [flag] shall be stored with the preserved data until that flag is removed, following which the data shall be destroyed as soon as reasonably possible.

7. Violations

Due to the potentially serious consequences of a violation of the procedures set out in this guide any violation may be subject to disciplinary action.

All members of staff or employees should report any suspected violations of this guide to the Data Compliance Manager.

8. Questions

Anyone with questions about this guide should contact the Data Protection Co-ordinator or the Data Compliance Manager.

CRANSLEY SCHOOL

DATA RETENTION SCHEDULE

1. Child Protection			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
1.1 Child Protection files	Education (Independent School Standards) Regulations 2014 applying the Education Act 2002 S 175[14]. "Record Keeping & Management of Child Protection Information - including guidance on consent" – Sept. 2011 & "Keeping Children Safe in Education – Sept. 2019" (KCSiE)	D.O.B + 25 years NOTE: IICSA HAS DECREED THAT SUCH DATA BE RETAINED INDEFINITELY UNTIL FURTHER NOTICE.	SECURE DISPOSAL unless legal action is pending
1.2 Allegation of a child protection nature against a member of staff, including where the allegation is unfounded.	"Keeping Children Safe in Education – Sept. 2019" (KCSiE)	Normally, until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer. HOWEVER, IICSA HAS DECREED THAT SUCH DATA BE RETAINED INDEFINITELY UNTIL FURTHER NOTICE.	SECURE DISPOSAL unless legal action is pending

2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.1 Details of all employees and dates of employment	Article 5 GDPR *("no longer than necessary"*)	7 years after termination of employment[15]	SECURE DISPOSAL unless legal action is pending
2.2 Employee offer letters, confirmation of employment letters, written particulars of employment, contracts of employment and changes to the terms and conditions	As above	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.3 Information on benefits per member of staff/employee	As above	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.4 Pension records	As above	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending

[14] The Education (Independent School Standards) Regulations 2014 apply the Education Act 2002 to independent schools. S 175 of the latter requires compliance with relevant guidance given by the Secretary of State – Statutory Guidance.

[15] The Information Commissioner considers this as acceptable on the basis that an employer is keeping information to protect against legal risk. Source – Pure Employment Law website.

2.5 Training records	As above	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.6 Job applications, CVs and interview records	ICO Employment Practices Code, Parts 1.7.5 and 1.7.6	7 months after notifying unsuccessful candidates; 6 years after termination of a successful employee.	SECURE DISPOSAL unless legal action is pending
2.7 Personnel Files (including all records relating to promotions, demotions, grievance procedures, resignation or termination letters	Article 5 GDPR *("no longer than necessary")*	7 years after termination of employment	SECURE DISPOSAL unless legal action is pending
2.8 Disciplinary Matters			
2.8.1 Verbal Warning Employment Relations Act	ACAS statutory Code of Practice on discipline and grievance issued under section 199 of the Trade Union and Labour Relations (Consolidation) Act 1992	Records resulting from a verbal warning should be retained on file for 6 months following the conclusion of disciplinary action, then destroyed[16].	SECURE DISPOSAL unless legal action is pending
2.8.2 Written Warning	As above	Records resulting from a written warning should be retained on file for 12 months following the conclusion of disciplinary action, then destroyed[17].	SECURE DISPOSAL unless legal action is pending
2.8.3 Final Written Warning	As above	Records resulting from a final written warning should be retained on file for 12 months following the conclusion of disciplinary action, then destroyed.	SECURE DISPOSAL unless legal action is pending
2.9 Job descriptions and performance goals	See section 2.1 & footnote 11	7 years after termination of employment[18]	SECURE DISPOSAL unless legal action is pending
2.10 Records in relation to hours worked and payments made to workers	National Minimum Wage Regulations 2015	3 years beginning with the day upon which the pay reference period immediately following that which they relate ends.	SECURE DISPOSAL unless legal action is pending
2.11 Records relating to accidents / injury at work			
2.11.1 Any death,	Reporting of Injuries,	7 years from date of	SECURE DISPOSAL unless

[16] Supplementary guidance to the ACAS Code of Practice on disciplinary and grievance procedures recommends a currency of 6 months for verbal warnings.
[17] Supplementary guidance to the ACAS Code of Practice on disciplinary and grievance procedures recommends a currency of 6 months for written warnings.
[18] The Information Commissioner considers this as acceptable on the basis that an employer is keeping information to protect against legal risk. Source – Pure Employment Law website.

specified injury, disease or dangerous occurrence & where a worker is away from work or incapacitated for more than three consecutive days	Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)	incident[19].	legal action is pending
2.11.2 Information relating to the member of staff's/employee's exposure to toxic substances for which medical surveillance is appropriate. (Medical Records to be stored separately in confidential location.)	Control of Substances Hazardous to Health Regulations 2002	At least 40 years from the individual leaving the school.	SECURE DISPOSAL unless legal action is pending
2.12 Working time opt-out form	The Working Time Regulations 1998	2 years from the date the record was made.	SECURE DISPOSAL unless legal action is pending
2.13 Records to show compliance with the Working Time Regulations 1998	The Working Time Regulations 1998	2 years after the date the record was made.	SECURE DISPOSAL unless legal action is pending
2.14 Annual leave record	HMRC Requirements.	7 years or possibly longer if leave can be carried over from year to year[20]	SECURE DISPOSAL unless legal action is pending
2. Employer Policies, Personnel Records, and Payroll Documents			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
2.15 Payroll and wage records for companies	HMRC Requirements.	7 years from the financial year end in which payments were made	SECURE DISPOSAL unless legal action is pending
2.16 Maternity records	Regulation 26, Statutory Maternity Pay (General) Regulations 1986	3 years after the end of the tax year in which the maternity pay period ends.	SECURE DISPOSAL unless legal action is pending
2.17 Current bank details	Article 5 GDPR *("no longer than necessary"*)	No longer than necessary.	SECURE DISPOSAL unless legal action is pending
2.23 Death benefit nomination and revocation forms	Article 5 GDPR *("no longer than necessary"*)	While employment continues or up to 6 years after payment of benefit.	SECURE DISPOSAL unless legal action is pending
2.18 Consents for the processing of personal and sensitive data	Article 5 GDPR *("no longer than necessary"*)	For as long as the data is being processed and up to 7 years afterwards	SECURE DISPOSAL unless legal action is pending
2.19 Disclosure and Barring Service checks and disclosures of criminal	Rehabilitation of Offenders Act 1974 & Rehabilitation of	Should be deleted following recruitment process unless assessed as	SECURE DISPOSAL unless legal action is pending

[19] RIDDOR states "at least 3 years from the date of the incident". This period is chosen to accommodate potential civil action.
[20] The Information Commissioner considers this as acceptable on the basis that an employer is keeping information to protect against legal risk. Source – Pure Employment Law website.

record forms	Offenders Act 1974 (Exceptions) Order 1975 as amended The Information Commissioner's Employment Practices Code, Parts 1.7.4 and 2.15.3	relevant to ongoing employment relationship. The information may include information on any spent conviction permitted under the exceptions order	
2.20 Emails - School staff	Article 5 GDPR *("no longer than necessary"*)	Mail is retained for 6 months after a member of staff leaves employment with Cransley School	SECURE DISPOSAL unless legal action is pending
2.21 Emails – Senior Management Team staff	Article 5 GDPR *("no longer than necessary"*)	Mail is retained for 10 years after a member of staff leaves employment with Cransley School	SECURE DISPOSAL unless legal action is pending
2.22 My Documents	Article 5 GDPR *("no longer than necessary"*)	Documents retained for 6 months after a member of staff leaves employment with Cransley School	SECURE DISPOSAL unless legal action is pending
2.23 Minutes of Governors meetings	Article 5 GDPR *("no longer than necessary"*) but may refer to any legal requirement.	6 years from date of meeting	SECURE DISPOSAL unless legal action is pending

3. Pupil records			
Basic File Description	**Statutory Provisions**	**Retention Period**	**Notes & Actions**
3.1 Admission Registers	Education (Pupil Registration) (England) Regulations 2006(S.I. 2006/1751, to which there are amendments not relevant to these Regulations.)	Date of last entry in the book (or file) + 6 years	SECURE DISPOSAL unless legal action is pending
3.2 Attendance Reports		Date of register + 6 years	SECURE DISPOSAL unless legal action is pending
3.3 Pupil Files Retained in Schools			
3.3.1 Primary		Transfer pupil files to the next school when the child	SECURE DISPOSAL unless legal action is pending

		leaves. All data except Alumni to be removed 6 years after pupil has left school.	
3.3.3 Pupil applicants who did not enrol		7 years after decision	SECURE DISPOSAL unless legal action is pending
3.3.4 Special Educational Needs files, reviews and Individual Education Plan		D.O.B. of the pupil + 25 years then review.	SECURE DISPOSAL unless legal action is pending
3.3.5 Any death, or an injury that arose out of or in connection with a work activity and the pupil was taken directly from the scene of the accident to hospital for treatment.	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	D.O.B. + 21 years.	SECURE DISPOSAL unless legal action is pending
3.3.6 Information relating to a pupil's exposure to toxic substances for which medical surveillance is appropriate. (Medical Records to be stored separately in confidential location.)	Control of Substances Hazardous to Health Regulations 2002	At least 40 years from the individual leaving the school.	SECURE DISPOSAL unless legal action is pending
3.3.7. Any other records relating to accidents / injury in school		D.O.B. + 21 years.	SECURE DISPOSAL unless legal action is pending
3.4 Examination Results			
3.4.1 Internal examination results		5 years from the leaving date of the cohort	SECURE DISPOSAL unless legal action is pending
3.4.2 External examination results		6 months after national publication of results	SECURE DISPOSAL
3.5 Special Education Needs			
3.5.1 Any other records created in the course of contact with pupils		As above	SECURE DISPOSAL unless legal action is pending
3.5.2 Statement maintained under the Children and Families Act 2014	SEN Code of Practice refers to the DPA. Aligned to the period ALL pupil records are kept.	D.O.B. of pupil + 25 years	SECURE DISPOSAL unless legal action is pending
3.5.3 Proposed statement or amended statement	As above	As above	SECURE DISPOSAL unless legal action is pending
3.5.4 Advice and information for parents regarding Educational needs	As above	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
3.5.5 Accessibility strategy	As above	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
3.6 School trips and similar			

3.6.1 Parental permission slips for school trips where there has been no major incident.		Conclusion of trip	SECURE DISPOSAL unless legal action is pending
3.6.2 Parental permission slips for school trips where there has been a major incident	Limitation Act 1980	D.O.B. of the pupil involved in the incident + 25 years. The permission slips for all pupils on the trip need to be maintained to show that the rules for all pupils had been followed	SECURE DISPOSAL unless legal action is pending
3.10 Pupil emails		6 months after pupil leaves the school	SECURE DISPOSAL unless legal action is pending
3.11 Pupils' My Documents		12 months after pupil leaves the school	SECURE DISPOSAL unless legal action is pending

4. Complaint Records			
Basic File Description	Statutory Provisions	Retention Period	Notes & Actions
4.1 Any data relating to a complaint, issue or potential complaint or issue relating to; - any pupil - the school - any act or omission of any member of staff or other employee or any contractor engaged by the school - anything which happened in or around any premises occupied by the school		During the period which the complaint or issue is investigated until final disposition of the matter and thereafter for a period of 7 years. DO NOT DESTROY OR DELETE UNLESS AND UNTIL DESTRUCTION HAS BEEN SPECIFICALLY APPROVED BY THE HEADMASTER	
4.2 Other e-mail any attachments and voice recording (unless other provisions of this guide apply requiring longer retention)		7 years after resolution	Subject to any, longer retention period which may be required under other provisions of this guide

5. Litigation			
Basic File Description	Statutory Provisions	Retention Period	Notes & Actions
5.1 Records relating to pending, threatened or reasonably anticipated litigation, government investigation, or complaint or other claim		During the period in which the litigation, investigation complaint or claim is contemplated, pending or threatened and until final disposition of the matter and thereafter for a period of 7 years. CHECK WITH Cransley School's Data Compliance Manager before destroying data	SECURE DISPOSAL unless legal action is pending

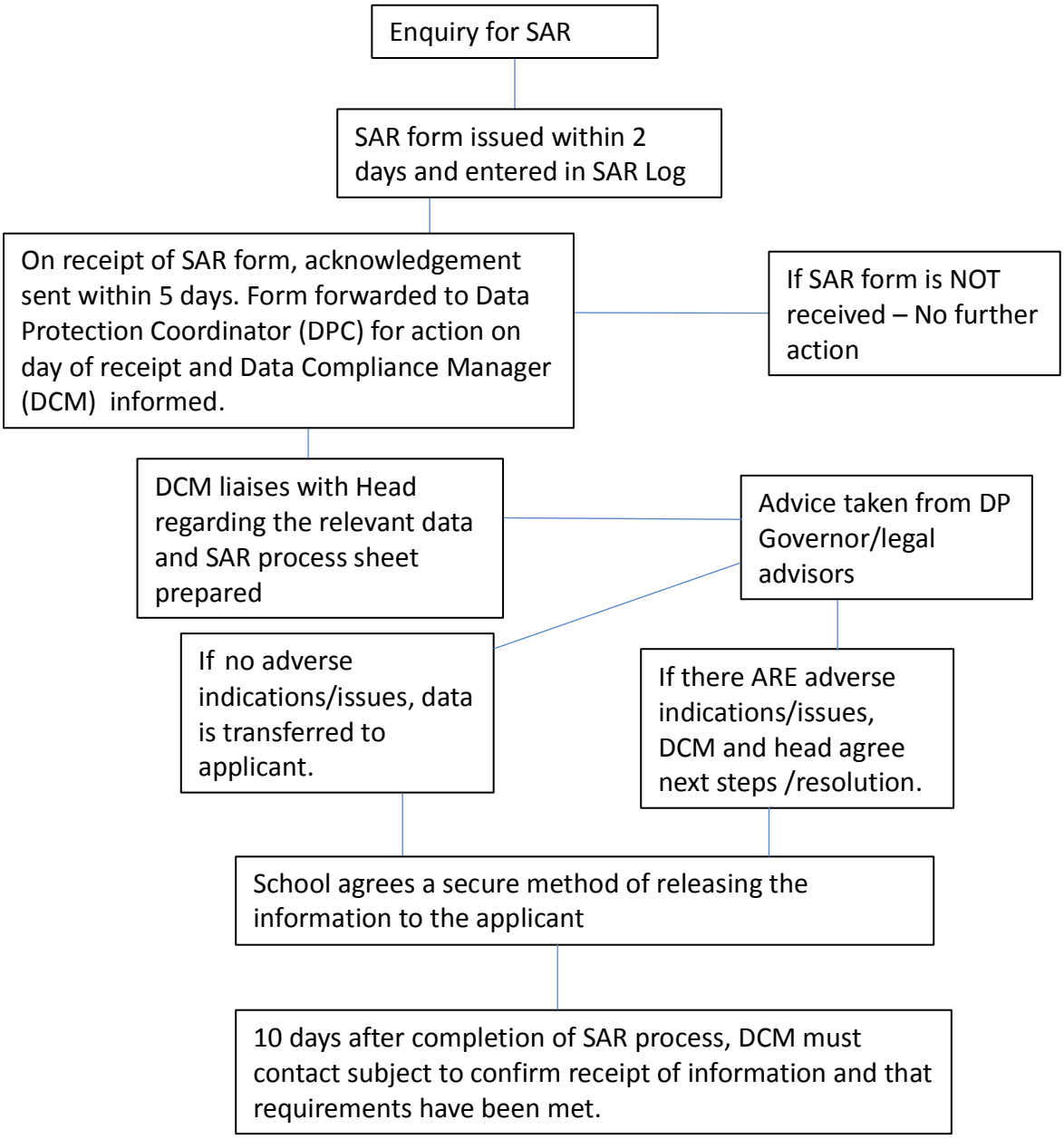
CRANSLEY SCHOOL

Appendix M : Data Disposal Log

DATE	DESCRIPTION	RECORDS INCLUDED	EXCEPTIONS
	Example: Annual audit of records in line with retention timescale or request from subject to change or delete record.		Individual pupils record as per retention log e.g. for legal proceedings ongoing etc.

CRANSLEY SCHOOL

Appendix N : SAR Flowchart



CRANSLEY SCHOOL

Appendix O : SAR Process Sheet

SAR reference:					
Date Acknowledged					
Target Date to DPA					
Target Date for Release					
Verification of Subject					
Date	**Description of document; letter / email / report incl. who from / to and 'cc' details.**	**Editing done and reasons given. E.g. Third parties anonymised.**	**Notes – check names for editing.**	**Copies Taken**	**Signature**
Correspondence (sections within the file are noted)					
Emails					
Sims					
Minutes of meetings					
Notes of visits					
Student File					
Accident Book					
Staff Personal File					
Sickness Records					
Other (Specify)					
Signature of DPC/DCM					
Date					
Space for clarifying notes:					

CRANSLEY SCHOOL

Appendix P : SAR Release Letter

[Name]
[Address]

[Date]

Dear [Name of data subject]

General Data Protection Regulation 2018: Subject Access Request

Thank you for your correspondence of [date] making a data subject access request for [subject]. We are pleased to enclose the information you requested. We have endeavoured to provide all the information that we hold on the data subject. However, if you have any reason to believe that there is any missing data then please do not hesitate to seek further clarity from us on this matter.

Yours Sincerely

CRANSLEY SCHOOL

Appendix Q : Confidentiality and Data Protection (v1)

Cransley School agrees to the <ABC> service operating a confidential service, namely < describe service> on our premises. Discussions between individual pupils and staff of <ABC> will remain confidential unless the young pupil of sufficient maturity[21] agrees to sharing, or there is an over-riding duty of care to the young person or someone else.

Pupils will be made aware of the confidential nature of this service by staff of <ABC> at their interventions. Pupils will also be asked by staff of <ABC> if, and what they may wish to share with the school, their parents or any third parties and their wishes will be respected.

As a Data controller as defined by the General Data Protection Regulation 2018, Cransley school takes the security of pupil data seriously and expects <ABC> to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Cransley School:

Name (please print):

Role:

Date:

Signed on behalf of <ABC>:

Name (please print):

Role:

Date:

[21] See Cransley School Data Protection Policy. Sufficient maturity: The Information Commissioner would regard a young person age 12 to be of sufficient maturity to exercise their rights under the GDPR. This includes the right to Consent or withhold consent to share. This is a general guide and it is recognised that some younger people may be sufficiently mature whereas some older people may not.

Appendix R : Confidentiality and Data Protection (v2)

Cransley School agrees to the <ABC> service operating a service on our premises. Cransley School recognises that <ABC> offers a confidential service in normal circumstances. However, the <ABC> service, when delivered on our premises, will be done so in line with the school's policy on confidentiality. The school will normally share information about the pupil's progress with the parent. It is only in exceptional circumstances where a conflict of interest may exist will the school consider withholding information. The <ABC> service when working with pupils on our premises will adhere to this 'open' policy.

Discussions between individual pupils and staff of <ABC> may be shared with the school and parents unless it is agreed that an exception can be made in a particular circumstance involving a pupil of sufficient maturity.[22] Pupils will be made aware of the open nature of this service by staff of <ABC> at their interventions.

As a Data Controller as defined by the General Data Protection Regulation 2018, Cransley School takes the security of pupil data seriously and expects <ABC> agency to implement appropriate security and other measures to safeguard pupils and their data in line with data protection legislation.

Confidentiality and data handling will form part of the review of this Service Level Agreement. Any concerns in this regard will be addressed by the personnel from each organisation.

Signed on behalf of Cransley School:

Name (please print):

Role:

Date:

Signed on behalf of <ABC>:

Name (please print):

Role:

Date:

[22] See Cransley School Data Protection Policy. Sufficient maturity: The Information Commissioner would regard a young person age 12 to be of sufficient maturity to exercise their rights under the GDPR. This includes the right to Consent or withhold consent to share. This is a general guide and it is recognised that some younger people may be sufficiently mature whereas some older people may not.

CRANSLEY SCHOOL

Appendix S : Data Protection Audit Return

Year:

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.0	Staff / Pupil Records					
1.1	Student data is kept in accordance with the data retention policy.					
1.2	Staff data is kept in accordance with the data retention policy.					
1.3	Expired records are disposed of safely and securely by named individuals.					
1.4	All forms used to collect data are identified					
1.5	All forms used to collect data refer to the Privacy Notice and the school's data protection policy.					
1.6	The Pupil Data Collection sheet (Appendix G) is sent out to parents, annually at a set time, to collect/refresh pupil data.					
1.7	All electronic databases in use, including the users who can access them, are identified.					
1.8	Access to all electronic databases is secured by individual username and password.					
1.9	All paper record systems in use, for staff or pupils, are identified.					
1.10	All paper record systems are secured in accordance with policy guidelines.					
1.11	Staff with access to staff records is documented, controlled and regularly reviewed.					
1.12	The standard Parent Contract is being used.					
1.13	The Accident Book is used for pupils and records are kept for 40 years from the date the incident is logged.					

1.14	The Accident Book is used for staff and records are kept for 40 years from the date the incident is logged.					
1.15	All pupils, whose parents have opted not to have their photograph used, are clearly identified with the information easily accessible to staff.					
2.0	Procedures					
2.1	All third party organisations offering a service on school premises, including the data they collect (if any), are identified.					
2.2	Are any 3rd party provider using Cloud based services? If so confirm you have discussed this with the DPC & IT advisors as indicated in the policy					
2.2	All Service Level Agreements with third party organisations are reviewed to consider data handling compliance.					
2.3	The school has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is documented and completed.					
2.4	Contact details of parents are not distributed to other parents, for legitimate school activities, unless a signed Parent Consent Form is received by the school (Appendix p of Data Protection Policy).					
2.5	A Subject Access Request (SAR) file is in place to store requests					
2.6	The SAR process has been tested. Please complete					

	Appendix B for a random pupil to test the process and outline any issues or concerns.					
3.0	Staff training					
3.1	Staff are made aware of Cransley School's Data Protection Policy and its implications for them in their work.					
3.2	Staff are made aware of Cransley School's Acceptable use of IT, mobile devices and social networking sites policy and its implications for them in their work.					
3.3	Staff are made aware of that they must inform the school of any changes to their personal details, e.g. change of address, contact numbers.					
3.4	Have you received staff DP training materials?					
3.5	Have all staff had the minimum training session?.					

Status Key:	
Status	Description
	Policy standard not met.
	Policy standard partially met. Action Plan in place to achieve full compliance
	Policy standard achieved.

Audit completed by (please print):

Signed:

Position:

Date: