CREST INFANT & NURSERY SCHOOL

Data Protection Policy

Person Responsible: Jane Shields

Date of Policy: May 2018
Date of this review: May 2020
Date of next review: May 2022

Contents:

Introduction

Crest Infant & Nursery School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the Local Authority (LA), other schools and educational bodies, and potentially social services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative and it is good practice to keep clear practical policies, backed up by written procedures.

1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner's Office (2017) „Overview of the General Data Protection Regulation (GDPR)"
- Information Commissioner's Office (2017) „Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now"

2. Applicable data

2.1. For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an online identifier such as an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible.

2.2. Sensitive personal data is referred to in the GDPR as "special categories of personal data", which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; having regard to the purposes for which data is processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

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

4. Accountability

4.1. Crest Infant & Nursery School will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The schools will provide clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures

4.5. The school will implement measures that meet the principles of data protection.

4.6. Data protection impact assessments will be used, where appropriate.

5. Data protection officer (DPO)

5.1. A DPO has been appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. An existing employee may be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the Head Teacher.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

The school's DPO is: **Andy Wilson**

6. Lawful processing

6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, all data will be lawfully processed using a Privacy Impact Statement (PIS) ***Appendix 5***

7. Consent

7.1. Consent must be a positive indication and will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. The consent of parents will be sought prior to the processing of a child's data, except where the processing is related to preventative or counselling services offered directly to a child.

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. ***Appendix 1&2.***

8.2. If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) ***Appendix 6*** to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The school will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the schools will impose a fee of £10.00 to comply with requests for further copies of the same information.

9.5. All requests will be responded to without delay and at the latest, within one month of receipt.

9.6. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.7. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.8. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible and details of the third parties.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

10.5. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. The schools have the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

11.5. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. The right to restrict processing

12.1. Individuals have the right to block or suppress the school's processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

12.3. The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The school will inform individuals when a restriction on processing has been lifted.

13. The right to data portability

13.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14. The right to object

14.1. The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice.

14.2. Individuals have the right to object to the following:
- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:
- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:
- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

15. Safeguarding and confidentiality

15.1 There will be instances where the school deems it necessary to share data with local authorities or the police where the child is considered at risk from harm, neglect or abuse. This may be carried out without consent if the circumstances justify it – where it is in the substantial public interest, and necessary for the purpose of:
- Protecting an individual from neglect or physical, mental or emotional harm; or
- Protecting the physical, mental or emotional well-being of an individual

15.2 The possibility of obtaining consent from an individual will be considered, but if in the circumstances the consent cannot be given, or the data controller cannot reasonably be expected to obtain it – notably because obtaining it would prejudice the safeguarding purpose (i.e. the protection of the individual) – then the data will be shared.

16. Data breaches

16.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

16.2. The Head Teacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their continuous development training.

16.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

16.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it. ***Appendix 5***

16.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

16.6. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school.

17. Data security (the following is incorporated into the staff code of conduct for data protection)

17.1. Confidential paper records will be kept in locked filing cabinets, drawers or safe, with restricted access.

17.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.
17.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
17.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
17.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
17.6. All electronic devices are password-protected to protect the information on the device in case of theft.
17.7. Staff will not use their personal laptops or computers for school purposes.
17.8. All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
17.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
17.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
17.11. When sending confidential information by fax, staff will always check that the recipient is correct before sending.
17.12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
17.13. Before sharing data, all staff members will ensure:
- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

17.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
17.15. The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
17.16. Crest Infant & Nursery School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18. Publication of information

18.1. Crest Infant & Nursery School publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:
- Policies and procedures
- Minutes of meetings

18.2. Classes of information specified in the publication scheme are made available quickly and easily on request.
18.3. Crest Infant & Nursery School will not publish any personal information, including photos, on its website without the permission of the affected individual.
18.4. When uploading information to the school website, staff are considerate of any data which could be accessed in documents and images on the site.

19. CCTV and photography

19.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
19.2. The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
19.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

19.4. All CCTV footage will be kept for a minimum length of time for security purposes (31 days).
19.5. The school will always indicate its intentions for taking photographs of pupils and will gain permission before publishing them.
19.6. If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
19.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

20. Data retention

20.1. Data will not be kept for longer than is necessary.
20.2. Unrequired data will be deleted as soon as practicable.
20.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
20.4. Paper documents will be shredded or placed into the confidential waste bins, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.
20.5 The transfer of data files e.g. pupil files. The school will ensure a checking system is in place. All pupil files will be checked by the Headteacher (or Deputy in her absence) before being sent to the receiving school. The responsible member of the admin team will then re-check the files and ensure each file is placed into an individual envelope.

21. DBS data

21.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
21.2. Data provided by the DBS will never be duplicated.
21.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

22. Review

22.1. This policy will be reviewed every two years.

Jane Shields
Data Controller

Initially approved at the Resources Committee of the Governing Body meeting on 17th May 2018

Ratified by the Full Governing Body at the meeting on 1st April 2020 (postponed to 20th May 2020)

Associated Documents:

- Safeguarding Policy
- E-Safety Policy
- Freedom of Information Policy

Date of next review: by May 2023

Appendix 1

General Privacy Notice - Data Protection Act 1998
We collect, use and store information about our pupils and may receive information about pupils from their previous school. This information helps us:

- support in the teaching and learning of our pupils;
- follow and report on the progress of our pupils;
- provide the right care and support for our pupils; and
- understand how well our school is doing as a whole.

The information we keep includes contact details; assessment marks and results; attendance records; other information such as ethnic group or religion; special educational needs; and any relevant medical information.

We will collect information about immediate family members for the purposes of communication and safeguarding. By providing such information, you are giving consent for the school to use this for its own direct communication purposes only.

We are required (under the Data Protection Act) to take care of all information and we take this responsibility seriously. We will not give information about you to anyone outside the school without your consent unless the law and our rules permit it. We are required by law to pass some of your information to the Local Authority (LA), and the Department for Education (DfE).

Safeguarding and confidentiality
There will be instances where the school deems it necessary to share data with local safeguarding authorities or the police where the child is considered at risk from harm, neglect or abuse. This may be carried out without consent if the circumstances justify it – where it is in the substantial public interest, and necessary for the purpose of:

- Protecting an individual from neglect or physical, mental or emotional harm; or
- Protecting the physical, mental or emotional well-being of an individual

The possibility of obtaining consent from an individual will be considered, but if in the circumstances the consent cannot be given, or the data controller cannot reasonably be expected to obtain it – notably because obtaining it would prejudice the safeguarding purpose (i.e. the protection of the individual) – then the data will be shared.

If you want to see a copy of the information we hold and share about you or your child, then please contact the school.

If you want more information about how the LA stores and uses this data, please contact:

Management Information Services
Medway Council
Gun Wharf
Dock Road
Chatham Kent ME4

For more information about how the DfE stores and uses this data, you can visit the following website: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Please contact the DfE if you would like a printed copy of the information:

Public Communications Unit: Department for Education
Sanctuary Buildings
Great Smith Street
London SW1P 3BT
Tel: 0370 000 2288
Website: https://www.gov.uk/government/organisations/department-for-education

Appendix 2

Workforce Privacy Notice - Data Protection Act 1998

The school workforce: those employed to teach, or otherwise engaged to work at, a school or a local authority

The Data Protection Act 1998: How we use your information

We process personal data relating to those we employ to work at, or otherwise engage to work at, our school. This is for employment purposes to assist in the running of the school and/or to enable individuals to be paid. The collection of this information will benefit both national and local users by:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling ethnicity and disability monitoring; and
- supporting the work of the School Teachers' Review Body

This personal data includes identifiers such as names and National Insurance numbers and characteristics such as ethnic group, employment contracts and remuneration details, qualifications and absence information.

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to pass on some of this personal data to:

- Medway Local Authority
- the Department for Education (DfE)

If you require more information about how we and/or DfE store and use your personal data please visit:

- www.medway.gov.uk
- https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

If you want to see a copy of information about you that we hold, please contact:

- Mrs J Lindfield (School Office Manager)
- Medway HR Team

Appendix 3

Privacy Impact Assessment

Complete for all new uses of personal data or existing high risk personal data. To be completed by the person who wants to use that service and signed off by the Data Protection Officer. This will then inform the data audit.

What is the aim of the project?			
What data will be collected?			
How will the data be collected?			
How will the data be stored?			
How will the data be shared?			
How will the data be amended or deleted?			
Identified risks (Issues, risks to individuals, compliance risk, school risk, possible solution)			
Signed off by:		Date:	

Appendix 4

Subject Access Request Record

Name of data subject	
Name of person making the request	
Date request received	
Contact DPO	Andy Wilson
Date acknowledgement sent	
Name of person dealing with request	

	Comments and notes
Are they entitled to the data?	
Do you understand what data has been requested?	
Identify the data.	
Collect the data required.	
Is there a need to exempt/redact any data?	
Create a pack.	
Inform the requestor you have the data.	
Deliver data.	

Date request completed (within 30 days of request)	
Signed off by:	

Appendix 5

Data Protection Breach Record

Date:		Person responsible for dealing with breach:				
Outline of breach						
Which data subjects are involved?						
Data type involved:						
Reported by?						
Phone/email sent to DPO.	Y / N	Is this risk high?	Y / N	Report to ICO	Y / N	
Date reported to the data subjects.						
Actions taken						
Preventative action suggestions – including training.						
Notes.						
Actions approved by:		Date:				

Consider content to be added to data collection sheets on enrolment.

Consent statement
All schools are required by law to keep on record details of pupils admitted. We must also obtain details of those with legal responsibility for the child.
All data collected will only ever be used within school for purposes for communication and analysis. Data will only be passed on by the school to the next school into which the child is enrolled. Data may also be passed on to local safeguarding authorities or the police in the event of any child protection or safeguarding concerns.

- By signing this form you are giving consent for the above.
- By providing your email address, you are giving consent for the school to provide email communications to you.