



# **The Crossley Heath School**

Savile Park, Halifax, West Yorkshire HX3 0HG

Tel: 01422 360272 • Fax: 349099 • email [admin@crossleyheath.org.uk](mailto:admin@crossleyheath.org.uk)

## **Data Protection Policy**

## Version Control

Version Number	Purpose/Change	Author	Date
1	Original Policy	Jonathan Lees	07/02/2018
1.1	Approved	Governors	03/07/2018
2	Reviewed	Jonathan Lees	24/11/2020
2	Submission to B&R Governors for Approval	Paula Oldroyd	23/03/2021
3	Reviewed	Jonathan Lees	02/03/2022
4	Ratified at B&R Committee		March 22

## Table of Contents

	Page No
Version Control	1
Statement of Intent	3
Legal Framework	3
Principles	4
Accountability	4
Data Protection Officer	5
Staff Training and Induction	6
Lawful Processing	6
Consent (Individuals)	7
The Right to be Informed (Individuals)	7
The Right of Access (Individuals)	8
The Right of Rectification (Individuals)	9
The Right of Erasure (Individuals)	10
The Exercise of defence of legal claims (Individuals)	10
The Right to Restrict Processing (Individuals)	10
The Right to Data Portability (Individuals)	11
The Right to Object (Individuals)	12
Automated Decision Making and Profiling (Individuals)	13

Privacy by Design and Privacy Impact Assessments	13
Data Breaches	14
Data Security	14
Publication of Information	16
CCTV and Photography	16
Data Retention	16
Policy Review	17

**Responsibility:** Data Protection Officer  
**Date of Review:** March 2024  
**Status:** Statutory

## 1. Statement of Intent

The Crossley Heath School Academy Trust Ltd 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) / Data Protection Act 2018.

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's 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 The Crossley Heath School Academy Trust Ltd believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR/Data Protection Act 2018, which came into effect on 25 May 2018.

## 2. Legal Framework

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

- The General Data Protection Regulation (GDPR) / Data Protection Act 2018
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulation 2004
- The School Standards and Framework Act 1998

2.2 This policy will also have regard to the following guidance:

- Information Commissioner's Office (ICO) (2018) 'Guide to the General Data Protection Regulation (GDPR)'

2.3 This policy will be implemented in conjunction with the following other school policies and plans:

- IT Security Policy
- CCTV Policy
- Photography and Videos at School Policy

- Clean Desk Policy
- Special Category Data Policy
- GDPR Data Security Breach Prevention and Management Plan

### **3. Applicable Data**

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, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

Sensitive personal data is referred to in the GDPR as ‘special categories of personal data’. These specifically include the processing of genetic data, biometric data and data concerning health matters.

### **4. Principles**

4.1 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- 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.

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

### **5. Accountability**

The Crossley Heath School Academy Trust Ltd will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

- 5.1 The school will provide comprehensive, clear and transparent privacy policies.
- 5.2 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.
- 5.3 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
  - Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- 5.4 The school will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Data minimisation.
  - Pseudonymisation.
  - Transparency.
  - Allowing individuals to monitor processing.
  - Continuously creating and improving security features.
- 5.5. Data protection impact assessments will be used, where appropriate.

## **6. Data Protection Officer (DPO)**

A DPO will be 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.
- 6.1 An existing employee will 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.
- 6.2 The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
- 6.3 The DPO will report to the highest level of management at the school, which is the Head Teacher.

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

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

## **7. Staff Training and Induction**

6.1 The school's DPO undertakes annual refresher training at two yearly intervals. The DPO also attends other opportunities such as any ICO webinars to ensure that they are up to date with current practices and procedures and to further their continuous professional development.

6.2 All other school staff undertake appropriate induction training to equip them to carry out their responsibilities for data protection effectively, which is kept up to date by refresher training at two yearly intervals. We ensure that this takes place through face-to-face delivery or by coordinating online training.

## **8. Lawful Processing**

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

8.1 Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks).

8.2 Sensitive data will only be processed under the following conditions and in line with the Special Category Data Policy:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:

- Carrying out obligations under employment, social security or social protection law, or a collective agreement.
- Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
- The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
- Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
- The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## **9. Consent (Individuals)**

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre ticked boxes.

- 9.1 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.
- 9.2 Where consent is given, a record will be kept documenting how and when consent was given.
- 9.3 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.
- 9.4 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 reobtained.
- 9.5 Consent can be withdrawn by the individual at any time.
- 9.6 Where a child is under the age of 16 the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

## **10. The Right to be Informed (Individuals)**

The privacy notice supplied to individuals in regard to the processing of their personal data will be written in clear, plain language, which is concise, transparent, easily accessible and free of charge.



- 10.1 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.
- 10.2 In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:
- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
  - The purpose of, and the legal basis for, processing the data.
  - The legitimate interests of the controller or third party.
  - Any recipient or categories of recipients of the personal data.
  - Details of transfers to third countries and the safeguards in place.
  - The retention period of criteria used to determine the retention period.
  - The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
  - The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
- 10.3 Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.
- 10.4 Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
- 10.5 For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.
- 10.6 In relation to data that is not obtained directly from the data subject, this information will be supplied:
- Within one month of having obtained the data.
  - If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
  - If the data are used to communicate with the individual, at the latest, when the first communication takes place.

## **11. The Right to Access (Individuals)**

- 11.1 Individuals have the right to obtain confirmation that their data is being processed.
- 11.2 Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

- 11.3 The school will verify the identity of the person making the request before any information is supplied.
- 11.4 A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
- 11.5 Where a SAR has been made electronically, the information will be provided in a commonly used electronic format unless requested differently.
- 11.6 Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.
- 11.7 All fees will be based on the administrative cost of providing the information if the request is deemed excessive.
- 11.8 All requests will be responded to without delay and at the latest, within one month of receipt.
- 11.9 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.
- 11.10 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.
- 11.11 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.

## **12. The Right to Rectification (Individuals)**

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

- 12.1 Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.
- 12.2 Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.
- 12.3 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 12.4 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.

### **13. The Right to Erasure (Individuals)**

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

13.1 Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

13.2 The school has 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

### **14. The Exercise or Defence of Legal Claims (Individuals)**

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.

14.1 Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

14.2 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.

### **15. The Right to Restrict Processing (Individuals)**

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

15.1 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.

15.2 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 processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

15.3 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.

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

## **16. The Right to Data Portability (Individuals)**

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

16.1 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.

16.2 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

16.3 Personal data will be provided in a structured, commonly used and machine-readable form.

16.4 The school will provide the information free of charge.

16.5 Where feasible, data will be transmitted directly to another organisation at the request of the individual.

16.6 The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

16.7 In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

16.8 The school will respond to any requests for portability within one month.

16.9 Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

16.10 Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

## **17. The Right to Object (Individuals)**

The Crossley Heath School Academy Trust Ltd will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

17.1 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.

17.2 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.

17.3 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.

17.4 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.

17.5 Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

## **18. Automated Decision Making and Profiling (Individuals)**

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

18.1 The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

18.2 When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

18.3 Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The school has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

## **19. Privacy by Design and Privacy Impact Assessments**

The Crossley Heath School Academy Trust Ltd will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

19.1 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school's data protection obligations and meeting individuals' expectations of privacy.

19.2 DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school's reputation which might otherwise occur.

19.3 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

19.4 A DPIA will be used for more than one project, where necessary.

19.5 High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

19.6 The school will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

19.7 Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

## **20. Data Breaches**

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. The Crossley Heath School Academy Trust Ltd is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions, and to have systems and procedures in place that support this.

The Crossley Heath School Academy Trust Ltd recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities, and to take steps to help prevent a repeat occurrence. This can be found in the schools’ GDPR Data Security breach prevention and management plan.

## **21. Data Security**

Access to personal data across The Crossley Heath School Academy Trust Ltd is a vital element for employees to be able to perform their duties. It is however under Data Protection law, a requirement that all staff protect personal data from unlawful disclosure or loss.

21.1 The Data Protection Officer will conduct a back-up of information on a daily basis to ensure that all data can still be accessed in the event of a security breach, e.g. a virus, and prevent any loss or theft of data.

- 21.2 Paper records containing personal information are kept in a locked filing cabinet, drawer or safe, with restricted access at all times and in line with the clear desk policy.
- 21.3 Paper records containing personal information records are not left unattended or in clear view when held in a location with general access and in line with the Clear desk policy.
- 21.4 Sensitive personal data that is stored on a shared network drive will be encrypted or password protected.
- 21.5 Where data is saved on removable storage or a portable device for backup purposes, the device is kept in a locked and fireproof safe when not in use.
- 21.6 Memory sticks are not allowed in school.
- 21.7 All mobile laptop devices are encrypted to protect the information on the device in case of theft.
- 21.8 Where possible, staff and governors should not use their personal laptops or computers for school purposes.
- 21.9 All members of staff are provided with their own secure login and password and must keep it safe at all times.
- 21.10 Emails containing sensitive or confidential information are password-protected if they are sent outside of school.
- 21.11 Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- 21.12 Where personal information that could be considered private or confidential is taken off the premises, to fulfil the purpose of the data in line with the GDPR, either in an electronic or paper format, staff 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.
- 21.13 Before sharing data with a third party, staff always ensure that:
- They have consent from data subjects to share it.
  - Adequate security is in place to protect it.
  - The data recipient has been outlined in a privacy notice.
- 21.14 All staff members will follow the 'Clear Desk Policy' to avoid unauthorised access to physical records containing sensitive or personal information.
- 21.15 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.



21.16 The physical security of the school's buildings and storage systems, and access to them, is reviewed annually by the Business manager in conjunction with the DPO. If an increased risk in vandalism, burglary or theft is identified, this will be reported to the headteacher and extra measures to secure data storage will be put in place.

21.17 All employed staff have responsibility for protecting personal data and taking the GDPR seriously. Any unauthorised disclosure or loss of data due to carelessness may result in disciplinary action.

21.18 The Data Protection Officer is responsible for continuity and recovery measures are in place to ensure the security of protected data.

21.19 Any damage to or theft of data will be managed in accordance with the school's Security Breach Management Plan.

## **22. Publication of Information**

The Crossley Heath School Academy Trust Ltd publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

22.1 Classes of information specified in the publication scheme are made available quickly and easily on request.

22.2 The Crossley Heath School Academy Trust Ltd will not publish any personal information, including photos, on its website without the permission of the affected individual.

22.3 When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

## **23. CCTV and Photography**

The Crossley Heath School Academy Trust Ltd understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles and in line with the schools' CCTV policy and Photography and Videos at School Policy.

## **24. Data Retention**

The Crossley Heath School Academy Trust Ltd is committed to maintaining the confidentiality of its information and ensuring that all records within the school are only accessible by the appropriate individuals. In line with the requirements of the General Data Protection Regulation (GDPR), the school also has a responsibility to ensure that all records are only kept for as long as is necessary to

fulfil the purpose(s) for which they were intended and has created the GDPR compliant Records Management policy to outline how records are stored, accessed, monitored, retained and disposed of, in order to meet the school's statutory requirements.

## **25. Policy Review**

This policy is reviewed every two years by the Data Protection Officer.