# Data Protection Strategy

**Document History**

| | |
|---|---|
| Version number | 5.2 |
| Approved by | Board of Trustees |
| Approval date | June 2023 |
| Adopted by | n/a |
| Adopted date | n/a |
| Implementation date | September 2023 |
| Policy/document owner | Data Protection Officer |
| Status | Statutory |
| Frequency of review | Every two years |
| Next review date | June 2025 |
| Applicable to | This policy applies to the Trust and all constituent schools. |

| Date | Author | Version Number | Summary of changes |
|---|---|---|---|
| 25 Feb 2018 | Director of Operations | V1 | New strategy – 1st Draft |
| 27 March 2018 | Director of Operations | V2 | Revised Policy following comments of CEO |
| 16 April 2018 | Director of Operations | V3 | Reviewed with Director of IT |
| 1st May 2018 | Director of Operations | V4 | Reviewed Governance structures |
| May 2020 | Head of Governance | V5 | Reviewed by Executive Team. Changes to general wording, formats and ordering of information. Additional sections added on responsibilities, storing personal data, procedure for responding to rights request and training. |
| November 2020 | Head of Governance | V5.1 | Updated branding |
| 12th June 2023 | Data Protection Officer | V5.2 | Reviewed all sections and updated where necessary. Changed all "staff" to "colleagues". Changed anything with "DSAT" to "Discovery". |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Contents:**

## Statement of intent

**Discovery School's Academy Trust,** further referred to as **Discovery, or the organisation** is required to keep and process certain information about its colleague's, members, and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The organisation may, from time to time, be required to share personal information about its colleagues or pupils with other organisations, mainly the LA, other trust schools and educational bodies, and potentially social services.

This strategy and accompanying polices are in place to ensure all colleagues and governors are aware of their responsibilities and outlines how the organisation complies with the following core principles of the GDPR.

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

This policy complies with the requirements set out in the GDPR and the Data Protection Act 2018.

Responsibility for the review of this Strategy and the related policies sits with the Finance, Audit and Risk Committee (FAR)

## 1. Aims

Discovery aims to ensure that all data collected about colleagues, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998.

This strategy and related policies apply to all data, regardless of whether it is in paper or electronic format.

## 2. Legal framework

2.1. This strategy also takes into account the expected provisions of the General Data Protection Regulation which is new legislation due to come into force on 25th May 2018 and has due regard to other legislation, including, but not limited to the following:

- 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

2.2. This strategy will be implemented in conjunction with the following trust policies:

- **Document Retention Management Policy**
- **ICT Acceptable Use Policy**
- **Mobile Phone and Loaned Equipment Policy**
- **Data Security Incident Management Policy**
- **Freedom of Information Policy**
- **CCTV Policy**
- **School Workforce Privacy Notice**
- **Parent/carer Privacy Notice**

2.3. This policy complies with our funding agreement and articles of association.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Personal data is any information relating to an identified or identifiable natural (living) person. |

| | |
|---|---|
| **Sensitive personal data (special category)** | Data such as:<br>• Contact details<br>• Racial or ethnic origin<br>• Political opinions<br>• Religious beliefs, or beliefs of a similar nature<br>• Where a person is a member of a trade union<br>• Physical and mental health<br>• Sexual orientation<br>• Whether a person has committed, or is alleged to have committed, an offence<br>• Criminal convictions |
| **Processing** | Obtaining, recording, holding data or shredding/deleting |
| **Data subject** | The person whose personal data is held or processed |
| **Data controller** | A person or organisation that determines the purposes for which, and the manner in which, personal data is processed. |
| **Data processor** | A person, other than an employee of the data controller, who processes the data on behalf of the data controller |

## 4. The Data Controller

Discovery processes personal information relating to pupils, colleagues, and visitors, and, therefore, is the **data controller**. Discovery delegates the responsibility of day-to-day management of data as data controller to Local Data Protection Representatives (LDPR) at each workplace location. See 7.2.

Discovery is registered as a data controller with the Information Commissioner's Office and renews registration annually.

## 5. Principles

5.1. 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.
- 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.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

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

## 6. Accountability

6.1. Discovery instructs all schools and its partner organisations to implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

6.2. Discovery will provide comprehensive, clear, and transparent privacy policies.

6.3. 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.

6.4. The organisation will implement measures in all locations that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Transparency.

- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

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

## 7. Data Protection Officer (DPO)

7.1. The organisation's DPO will offer advice, guidance and a bespoke quality assurance provision that meets the needs of Discovery and GDPR regulations. The DPO will work with the Director of IT and the Director of Operations to:

- Inform and advise schools and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the organisation's compliance with the GDPR and other laws, including quality assuring internal data protection activities, advising on data protection impact assessments, conducting annual internal audits, and providing the required training to colleagues.

7.2. Day-to-day data management and operational responsibilities rest with the Local Data Protection Representatives (LDPR) who in the main will be the Office Manager or School Business Manager in schools and key personnel within the partner organisations; SCITT and EPIC. The LDPR will assist the DPO in ensuring that all colleagues are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

7.3. All colleagues are responsible for ensuring that they collect and store any personal data in accordance with this strategy and related policies. Colleagues must also inform their workplace of any changes to their personal data, such as a change of address.

7.4. The DPO will report annually to the highest level of management of the trust, which is the **Board of Trustees** through the Finance, Risk and Audit Committee (FAR)

7.5. The DPO will operate independently and will not be penalised for performing their task.

7.6. Sufficient resources and support will be provided to the DPO to enable them to meet their GDPR obligations.

## 8. Lawful processing

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

Pupils and Parents.

- We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data

about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

- This data includes, but is not restricted to:
    - Contact details
    - Results of internal assessment and externally set tests
    - Data on pupil characteristics, such as ethnic group or special educational needs
    - Exclusion information
    - Details of any medical conditions

Colleagues

- We process data relating to those we employ to work within, or otherwise engage to work within, our organisation. The purpose of processing this data is to assist in the running of Discovery, including to:
    - Enable individuals to be paid
    - Facilitate safe recruitment
    - Support the effective performance management of colleagues
    - Improve the management of workforce data across the sector
    - Inform our recruitment and retention policies
    - Allow better financial modelling and planning
    - Enable ethnicity and disability monitoring
    - Support the work of the School Teachers' Review Body

Colleague's personal data includes, but is not limited to, information such as:

- Contact details
- National Insurance numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information

- Outcomes of any disciplinary procedures

8.2. 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 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.

8.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject,
- 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.
  - 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 of a contract with a health professional.
  - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

## 9. Consent

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

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

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

9.4. The trust 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.

9.5. 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 reobtained.

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

9.7. The consent of parents will be sought prior to the processing of a child's data, e.g photographic images for marketing purposes. Except where the processing is related to preventative or counselling services offered directly to a child.

## 10. The right to be informed

10.1. 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.

10.2. 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 the ICO.
- 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 and the details of the categories of personal data, 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 source 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 of access ('Subject Access Request')

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 organisation 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 organisation 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.

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.

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

11.10. Where a request is manifestly unfounded or excessive, the organisation 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 ICO,one month of the refusal.

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

## 12. The right to rectification

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

12.2. Where the personal data in question has been disclosed to third parties, the organisation will inform them of the rectification where possible.

12.3. Where appropriate, the organisation will inform the individual about the third parties that the data has been disclosed to.

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

12.5. Where no action is being taken in response to a request for rectification, the organisation will explain the reason for this to the individual and will inform them of their right to complain to the ICO.

## 13. The right to erasure ('right to be forgotten')

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

13.2. 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

13.3. The organisation 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
- The exercise or defence of legal claims

13.4. 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.

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

## 14. The right to restrict processing

14.1. Individuals have the right to block or suppress the organisations processing of personal data.

14.2. In the event that processing is restricted, the organisation 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.

14.3. The organisation 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 organisation has verified the accuracy of the data
- Where an individual has objected to the processing and the organisation 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 organisation no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim

14.4. If the personal data in question has been disclosed to third parties, the trust/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.

14.5. The organisation will inform individuals when a restriction on processing has been lifted.

## 15. The right to data portability

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

15.2. 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.

15.3. 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

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

15.5. The organisation will provide the information free of charge.

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

15.7. Discovery Schools Academies Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

15.9. The organisation will respond to any requests for portability within one month.

15.10. 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.

15.11. Where no action is being taken in response to a request, the organisation 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 ICO.

## 16. The right to object

16.1. 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 and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

16.2. 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.

16.3. 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 organisation 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.

16.4. Where personal data is processed for direct marketing purposes:

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

16.5. 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 organisation is not required to comply with an objection to the processing of the data.

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

## 17. Privacy by design and privacy impact assessments

17.1. Discovery will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the organisation has considered and integrated data protection into processing activities.

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

17.3. DPIAs will allow the organisation to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to Discovery Schools Academies Trust's reputation which might otherwise occur.

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

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

17.6. 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

17.7. The trust 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

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

## 18. Data breaches

18.1. 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. Guidance is found in the **Data Security and Incident Management Policy and Process** document.

18.2. The Data Protection Officer, Director of Operations and Director of IT will ensure that all LDPR's cascade information to all colleagues, to ensure they are made aware of, and understand, what constitutes as a data breach as part of their continuous development training.

18.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the Information Commission Office (ICO) will be informed.

18.4. All notifiable breaches will be reported to the ICO within 72 hours of the school becoming aware of it.

18.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis following the **Data Security and Incident Management Policy and Process**.

18.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Discovery will notify those concerned directly.

18.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the ICO.

18.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.9. Effective and robust breach detection, investigation and internal reporting procedures are in place throughout the trust, which facilitate decision-making in relation to whether the ICO or the public need to be notified. This is further discussed and procedures for managing Data Security Incidents included in the. **Data Security Incident Management Policy**

18.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO and other key personnel who may give support
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

18.11. Failure to report a breach when required could result in a fine, as well as a fine for the breach itself.

## 19. Data security

19.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3. Digital data is either coded, encrypted and/or password-protected, both on a local hard drive and on a network drive that is regularly backed up securely either on site or off-site.

19.4. Pen Drive (memory sticks) will not be used to hold personal information. Colleagues will use SharePoint to hold personal information securely.

19.5. All electronic devices are password-protected to protect the information on the device in case of theft.

19.6. Where possible, Discovery enables electronic devices to allow the remote blocking or deletion of data in case of theft.

19.7. Colleagues will not use their personal laptops or home computers for school purposes.

19.8. Governors will adhere to BYOD policy and related guidance when using personal laptops or home computers for Discovery governance business.

19.9. All colleagues are provided with their own secure login and password, and every computer regularly prompts users to change their password.

19.10. Emails sent outside the organisation which contain sensitive or confidential information or attachments are encrypted.

19.11. If circular emails to parents are used they are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients OR 3rd party communication providers are used.

19.12. In the infrequent case of sending confidential information by fax, colleagues will always check that the recipient details are correct and that they are aware of incoming communication before it is sent.

19.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, colleagues 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.

19.14. Before sharing data, all colleagues 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.

19.15. 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.

19.16. The physical security of the organisations 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.

19.17. Discovery takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.18. The **DPO** supported by the **Director of Operations** and **Director of IT** is responsible for ensuring that continuity and recovery measures are in place to safeguard the security of protected data.

## 20. Publication of information

20.1. Discovery publishes key statutory requirements on its website outlining different types of information that will be made routinely available, including:

- Policies and procedures
- Annual reports
- Financial information

20.2. Discovery will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.3. When uploading information to any of the organisations websites, colleagues are considerate of any metadata or deletions which could be accessed in documents and images on the site

## 21. CCTV and photography

21.1. Discovery understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. Discovery notifies all pupils, colleagues, and visitors of the purpose for collecting CCTV images via signage, notice boards, letters and/or email and adheres to the organisations **CCTV Policy** at all times.

21.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4. All CCTV footage will be kept for a maximum of **31 days** for security purposes, where applicable all **LDPR** are responsible for ensuring the records secure and allowing access.

21.5. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

21.6. If the organisation wishes to use images/video footage of pupils in a publication, such as a website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

21.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

## 22. Data retention

22.1. Data will not be kept for longer than is necessary in will adhere to the Discovery Document Retention Management Policy.

22.2. Unrequired data will be deleted as soon as practicable.

22.3. Some educational records relating to former pupils or employees of the organisation may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

22.4. Paper documents will be shredded, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

## 23. DBS data

23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Data provided by the DBS will never be duplicated.

23.3. 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.

## 24. Policy review

24.1. This policy is reviewed every two years by the Data Protection Officer and the Executive Team and adopted by the Finance Audit and Risk Committee

The next scheduled review date for this policy is June 2025