



# DATA PROTECTION POLICY

## Document Control

Description	By Whom	Date
Established (in line with 2018 DPA)	CB (DPO)	May 2018
Latest Review	CB / WM	Feb 24
Approved by Trustees	Andrew McCully – Chair of Trustees	March 24 Board meeting
Next Full Review due		Mar 25

# Table of Contents

About This Policy - Summary.....	3
Legislation .....	4
General Statement of Duties.....	4
Data Protection Officer .....	5
The Data Protection Principles.....	5
The Lawful Processing of Data .....	5
Types of Personal Data Processed By the Trust .....	6
Use of Personal Data by the Trust.....	7
Keeping In Touch and Supporting the Trust.....	7
Rights of Access to Personal Data ('Subject Access Request') .....	7
Exemptions .....	8
Whose Rights? .....	9
Disclosure of Information.....	9
Accuracy.....	10
Timely Processing.....	10
Enforcement .....	10
Data Security.....	10
Data Breaches .....	11
Categories of Data Loss .....	12
Complaints .....	12
Requests for Amendments of Data .....	12
Transparency and Accountability.....	12
Trust Website.....	13
Introducing a New Initiative or Project : Data Protection Impact Assessments .....	13
The Trust's Rights to Refuse a Request .....	14
Charges .....	14
Generic Policies.....	14
Training for Staff .....	14
On-going Guidance and Support for Staff .....	14
Equality Impact Assessment.....	15
Data Protection Statement .....	15
APPENDIX A – Data Protection policy checklist.....	17
APPENDIX B – Flowchart for requesting erasure / amendment of data.....	18
APPENDIX C – Key Data Management Links.....	19
APPENDIX D – Further guidance to support the implementation of this policy.....	20

## About This Policy - Summary

- The Harmony Trust, (including all Academies within it), collect and use personal information about staff, pupils, parents and other individuals who come into contact with the it. This information is gathered to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with their statutory obligations.
- Everyone has rights regarding how their personal data is handled. It is recognised that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations. Those who are involved in the processing of personal data are obliged to comply with this Policy when doing so. Any breach of this Policy may result in disciplinary action.
- This Policy sets out the basis on which the Trust and its Academies will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.
- This policy should be read in conjunction with the Information Management and Retention policy and the Biometric data policy.

### Contents of relevant data policies are as follows:

Data Protection policy	Information Management and Retention policy	Biometric data policy
<ul style="list-style-type: none"> <li>• Legislation</li> <li>• Roles and responsibilities related to Data Protection</li> <li>• Data protection principles</li> <li>• Reasons for lawfully processing data</li> <li>• Types of data</li> <li>• Rights of access to data (subject access requests)</li> <li>• Data security</li> <li>• Data breaches</li> <li>• Complaints</li> <li>• Data Protection Impact Assessments</li> <li>• Training requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Responsibilities with regards to information management</li> <li>• Storage</li> <li>• Email</li> <li>• Confidentiality</li> <li>• Auditing</li> <li>• Retention</li> <li>• Data transfer</li> <li>• Disposal</li> </ul>	<ul style="list-style-type: none"> <li>• Policy specifically regarding biometric data</li> <li>• Data protection principles, responsibilities and expectations related to biometric data</li> </ul>
<p><b>Appendices</b></p> <ul style="list-style-type: none"> <li>• <b>Checklist for Principals to ensure they are in line with the policy</b></li> <li>• Flowchart for requesting amendment / erasure</li> <li>• Data management links</li> <li>• Additional guidance and support to help apply the policy</li> </ul>	<p><b>Appendices</b></p> <ul style="list-style-type: none"> <li>• Specific timescales for the retention of different types of data</li> </ul>	

## Legislation

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

- UK General Data Protection Regulation 2021
- Protection of Freedoms Act 2012
- Freedom of Information Act 2000
- Limitation Act 1980 (as amended by the Limitation Amendment Act 1980)
- Data Protection Act 2018
- The Education Regulations (Educational Reports) 2005
- Information Records Management Society 'Information Management Toolkit for Academies' 2020

## Associated Policies

- This policy should be read in conjunction with the Online Safety Policy, Data Retention policy and the Biometric data policy.

## General Statement of Duties

The Trust is required to process relevant personal data regarding individuals as part of its operation and shall take all reasonable steps to do so in accordance with this Policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data.

The key responsibilities of the Trust in relation to data management are:

- To maintain its records and records managementsystems in accordance with legislation.
- The Principal at each academy is responsible for ensuring this policy is implemented and that all records are stored securely, in accordance with the retention periods outlined, recorded, and are disposed of correctly.
  - Ensuring that all records have an identified Information Asset Owner (IAO) whose responsibility it is to ensure records are managed in accordance with Trust Data Protection Policies and the UK GDPR.
  - To maintain an Information Asset Register. The Data Protection Officer will provide support and guidance to individual academies to ensure this is kept up to date. Maintaining the RoPA should not be a one-off activity and the document needs to be regularly reviewed. The Principal may delegate to the Data Protection Lead in their school the responsibility for maintaining the information asset register (IAR) and the record of processing activity (RoPA) in accordance with per Article 30 of UK GDPR and steps 2–5 of the Department for Education (DfE) Data Protection Toolkit for Schools.
  - Ensure records containing Personally Identifiable Information (PII) must be logged in the schools system to ensure the school meets its obligations under the UK GDPR to have a current data map. This information must be reviewable by the academy's Data Protection Lead to ensure that data sources are managed in line with policy and can be identified in the event of a Data Subject Access Request.
  - Ensure that staff are responsible for ensuring that any records for which they are responsible or which they process are accurate, maintained securely and disposed of correctly, in linewith the provisions of this policy.
  - That each academy within the Trust is individually responsible for the management of their records generated by its activities.
  - Its HR procedures will ensure managed access to systems and records. This should

include limits on how users access the resources, which user actions can be performed, and what resources users can access. Where individuals are given access to personal or sensitive data, training will be provided to ensure that they are aware of the increased risks, responsibilities (including confidentiality responsibilities), and the consequences of unauthorised access.

The Data Protection Officer will conduct an information audit on a regular basis with the academy's Data Protection Lead against all information held by the Trust and each academy to evaluate the information each is holding, receiving and using, and to ensure that this is correctly managed in accordance with the GDPR. The audit may involve interviews or questionnaires with key operational staff to identify information and information flows which may include the following:

- Paper documents and records
- Electronic documents and records (including emails)
- Databases
- Sound recordings
- Video and photographic records
- Hybrid files, containing both paper and electronic information
- Archives and archive logs

### **Data Protection Officer**

The Trust Data Protection Officer is responsible for providing guidance and advice on good records management practice and promoting compliance with this policy. Such guidance is formulated within the context of existing Trust policies and guidelines regarding data protection, national legislation and sector-wide standards.

- The Trust has appointed Colin Bellis, Illuminate Education Services UK Ltd, who will endeavour to ensure that all personal data is processed in compliance with this Policy and the principles of the Act. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the DPO.

### **The Data Protection Principles**

- Anyone processing personal data must comply with the eight enforceable principles of good practice as enshrined within the requirements of the DPA.
- These provide that personal data must be:
  - Fairly and lawfully processed
  - Processed for a lawful purpose
  - Adequate, relevant and not excessive
  - Accurate and up-to-date
  - Not kept for longer than necessary
  - Processed in accordance with the data subject's rights
  - Secure
  - Not transferred to other countries without adequate protection

### **The Lawful Processing of Data**

The UK GDPR and the Data Protection Act (2018) require all organisations to process data in a legal manner. In doing so, the lawful basis upon which each activity is processed must be made clear and clearly stated.

The six lawful grounds on which we can process data are:

1. Consent
2. Contract
3. Legal Obligation
4. Vital Interests (To Protects Someone's Life)
5. Public Task (a task in the public interests with a legal basis in law)
6. Legitimate Interests

### **Types of Personal Data Processed By the Trust**

Personal data covers both facts and opinions about an individual. The Trust may process a wide range of personal data about individuals including current, past and prospective pupils and their parents (as well as staff) as part of its operation, including, by way of example:

- Names, addresses, telephone numbers, email addresses and other contact details
- Bank details and other financial information, e.g. about parents who pay fees to the Trust
- Past, present and prospective pupils' academic, disciplinary, admissions and attendance records (including information about any special needs), and examination scripts and marks
- Where appropriate, information about individuals' health, and contact details for their next of kin
- References given or received by the Trust about pupils, and information provided by previous educational establishments and/or other professionals or organisations working with pupils; and
- Images of pupils (and occasionally other individuals) engaging in Trust activities, and images captured by Academy CCTV systems (in accordance with the Trust's policy on taking, storing and using images of children)
- Generally, the Trust receives personal data from the individual directly (or, in the case of pupils, from parents). However in some cases personal data may be supplied by third parties (for example another school, or other professionals or authorities working with that individual), or collected from publicly available resources

### **Sensitive Personal Data**

The Trust may, from time to time, need to process sensitive personal data regarding individuals. Sensitive personal data includes information about an individual's physical or mental health, race or ethnic origin, political or religious beliefs, sexual orientation, trade union membership or criminal records and proceedings. Sensitive personal data is entitled to special protection under the Act, and will only be processed by the Trust with the explicit consent of the appropriate individual, or as otherwise permitted by the Act. The consent should be informed, which means it needs to identify the relevant data, why it is being processed and to whom it will be disclosed. Staff should contact the DPO for more information on obtaining consent to process sensitive personal data.

#### **Processing Biometric Data**

- Specific guidance on the rights of staff and pupils with regard to the processing of biometric data is outlined in the Trust's Biometric Data policy.

## Use of Personal Data by the Trust

The Trust will use (and where appropriate share with third parties) personal data about individuals for a number of purposes as part of its operations, including as follows:

- For the purposes of pupil selection and to confirm the identity of prospective pupils and their parents
- To provide education services (including SEN), career services, and extra-curricular activities to pupils; monitoring pupils' progress and educational needs; and maintaining relationships with alumni and the Trust community
- For the purposes of management planning and forecasting, research and statistical analysis, and to enable the relevant authorities to monitor the Trust's performance;
- To give and receive information and references about past, current and prospective pupils, including relating to outstanding fees or payment history, to/from any educational institution that the pupil has attended or where it is proposed they attend
- To enable pupils to take part in national or other assessments, and to publish the results of public examinations or other achievements of pupils of the Trust
- To safeguard pupils' welfare and provide appropriate pastoral (and where necessary, medical) care, and to take appropriate action in the event of an emergency or accident, including by disclosing details of an individual's medical condition where it is in the individual's interests to do so, for example for medical advice, insurance purposes or to organisers of Trust trips;
- To monitor (as appropriate) use of the Trust's IT and communications systems in
- accordance with the Trust's Computing and Acceptable Use and Online Safety Policies
- To make use of photographic images of pupils in Trust publications, on the Trust
- website and (where appropriate) on the Trust's social media channels in accordance with the Trust's policy on taking, storing and using images of children
- For security purposes, and for regulatory and legal purposes (for example safeguarding and child protection and health and safety) and to comply with its legal obligations; and
- Where otherwise reasonably necessary for the Trust's purposes, including to obtain appropriate professional advice and insurance for the Trust

## Keeping In Touch and Supporting the Trust

The Trust may use the contact details of parents, alumni and other members of the Trust community to keep them updated about the activities of the Trust, including by sending updates and newsletters, by email and by post. Unless the relevant individual objects, the Trust may also:

- Share personal data about parents and/or alumni, as appropriate, with organisations set up to help establish and maintain relationships with the Trust community.
- Contact parents and/or alumni by post and email in order to promote and raise funds for the Trust and, where appropriate, other worthy causes
- Should you wish to limit or object to any such use, or would like further information about them, please contact the DPO in writing

## Rights of Access to Personal Data ('Subject Access Request')

Individuals have the right under the Act to access to personal data about them held by the Trust, subject to certain exemptions and limitations set out in the Act. Any individual wishing to access their personal data should put their request in writing to the DPO. The Trust will endeavour to respond to any such written requests as soon as is reasonably practicable and, in any event, within statutory time limits (one month).

- It should be noted that certain data is exempt from the right of access under the Act. This may include information which identifies other individuals or information which is subject to legal professional privilege. The Trust is also not required to disclose any pupil examination scripts (though examiners' comments may be disclosed), nor any reference given by the Trust for the purposes of the education, training or employment of any individual.
- The DPA states that pupils under the age of 16 are to be considered as 'vulnerable' and therefore are not allowed to amend their own data. As all our pupils are aged 12 and under, all subject access requests from pupils will therefore not be considered.
- Only a person with parental responsibility will generally be entitled to make a subject access request on behalf of younger pupils. A pupil of any age may ask a parent or other representative to make a subject access request on their behalf. In line with the DPA, we recognise the following rights in relation to data:

### **1. Right of Access.**

Individuals have the right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to that personal data.

### **2. Right to Rectification.**

Individuals have the right to obtain rectification of inaccurate personal data and the right to provide additional personal data to complete any incomplete personal data.

### **3. Right to Erasure ("Right to be Forgotten").**

In certain cases, individuals have the right to obtain the erasure of their personal data.

### **4. Right to Restriction of Processing.**

Individuals have the right to obtain a restriction of processing, applicable for a certain period and/or for certain situations.

### **5. Right to Data Portability.**

Individuals have the right to receive their personal data and they have the right to transmit such personal data to another controller.

### **6. Right to Object.**

In certain cases, individuals have the right to object to processing of their personal data, including with regards to profiling. They have the right to object at further processing of their personal data in so far as they have been collected for direct marketing purposes.

### **7. Right to be Not Subject to Automated Individual Decision-Making.**

Individuals have the right to not be subject to a decision based solely on automated processing.

### **8. Right to Filing Complaints.**

Individuals have the right to file complaints about the processing of their personal data with the relevant data protection authorities.

### **9. Right to Compensation of Damages.**

In case of a breach of the applicable legislation on processing of (their) personal data, individuals have the right to claim damages that such a breach may have caused with them.

## **Exemptions**

Certain data is exempted from the provisions of the Act, including the following:

- The prevention or detection of crime



- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Trust
- Information which might cause serious harm to the physical or mental health of the pupil or another individual
- Cases where the disclosure would reveal a child is at risk of abuse
- Information contained in adoption and parental order records
- Information given to a court in proceedings under the Magistrates' Courts (Children and Young Persons) Rules 1992
- Copies of examination scripts; and
- Providing examination marks before they are officially announced

The Trust will generally not be required to provide access to information held mutually and in an unstructured way.

Further exemptions may include information which identifies other individuals, information which the Trust reasonably believes is likely to cause damage or distress, or information which is subject to legal professional privilege. The Trust will also treat as confidential any reference given by the Trust for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. The Trust acknowledges that an individual may have the right to access a reference relating to them received by the Trust. However, such a reference will only be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent or if disclosure is reasonable in all the circumstances.

The above are examples only of some of the exemptions under the Act. Any further information on exemptions should be sought from the DPO.

### **Whose Rights?**

- The rights under the Act are those of the individual to whom the data relate. However, the Trust will, in most cases rely on parental consent to process data relating to pupils (if consent is required under the Act) unless, given the nature of the processing in question, and the pupil's age and understanding, it is more appropriate to rely on the pupil's consent. Parents should be aware that in such situations they may not be consulted.
- In general, the Trust will assume that pupils consent to disclosure of their personal data to their parents, e.g. for the purposes of keeping parents informed about the pupil's activities, progress and behaviour, and in the interests of the pupil's welfare, unless, in the Trust's opinion, there is a good reason to do otherwise.
- However, where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents, the Trust will maintain confidentiality unless, in the Trust's opinion, there is a good reason to do otherwise; for example where the Trust believes disclosure will be in the best interests of the pupil or other pupils.
- Pupils are required to respect the personal data and privacy of others, and to comply with the Trust's Acceptable Use and Online Safety Policies and any related Trust rules.

### **Disclosure of Information**

The Trust may receive requests from third parties to disclose personal data it holds about pupils, their parents or guardians. The Trust confirms that it will not generally disclose information unless the individual has given their consent or one of the specific exemptions under the Act

applies. However, the Trust does intend to disclose such data as is necessary to third parties for the following purposes:

- To give a confidential reference relating to a pupil to any educational institution which it is proposed that the pupil may attend
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend
- To publish the results of public examinations or other achievements of pupils of the Trust
- To disclose details of a staff or pupil's medical condition where it is in their interest to do so, for example for medical advice, insurance purposes or to organisers of Trust trips.
- To disclose details of a staff or pupil's medical condition where it is required as part of emergency arrangements (e.g. in a pandemic)
- Where the Trust receives a disclosure request from a third party it will take reasonable steps to verify the identity (and entitlement) of that third party before making any disclosure.

### **Accuracy**

The Trust will endeavour to ensure that all personal data held in relation to an individual is as up-to-date and accurate as possible. Individuals must notify the Academy or DPO of any changes to information held about them. An individual has the right to request that inaccurate information about them is erased or corrected (subject to certain exemptions and limitations under the Act) and may do so by contacting the DPO in writing.

### **Timely Processing**

The Trust will not keep personal data longer than is necessary for the purpose or purposes for which they were collected and will take all reasonable steps to destroy, or erase from its systems, all data which is no longer required. Guidance can be found in the Retention of Documents policy and accompanying guidance.

### **Enforcement**

If an individual believes that the Trust has not complied with this Policy or acted otherwise than in accordance with the Act, they should utilise the Trust's complaints procedure and should also notify the DPO.

### **Data Security**

- The Trust will take appropriate technical and organisational steps to ensure the security of
- personal data about individuals, and to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties under the Act.
- The Trust must ensure that appropriate security measures are taken against unlawful or
- unauthorised processing of personal data, and against the accidental loss of or damage to
- personal data. Accordingly, no member of staff is permitted to remove personal data from Trust premises, whether in paper or electronic form and wherever stored, without prior consent of the Principal. Where a member of staff is permitted to take data offsite it must be encrypted.

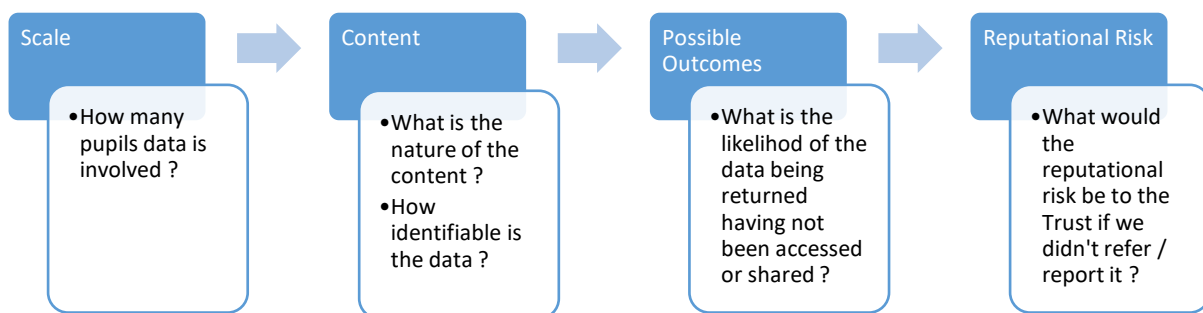
As a general principle, the Trust favours electronic storage of information, in order to:

- Assist data sharing where appropriate
- Ensure access to information by authorised users
- Ensure availability of information in the event of disaster recovery or business continuity

- Minimize duplication of data e.g. information stored in a school’s management information system will not also be printed and stored in a paper file.
  - The Trust’s Acceptable Use Policy for Staff details measures to ensure safe and secure storage and access to electronic records and should be read in conjunction with this policy.
  - Schools must ensure that key information is securely stored and can still be accessed in the event of a data breach including loss of access due to fire or flood or malware, to limit any loss or theft of data.
  - It is strongly recommended that schools should store key information in DfE approved enterprise-level cloud storage (Microsoft Office One Drive) to ensure access in the event of school closures.
  - Confidential paper records must be kept in a locked filing cabinet, drawer or safe, with restricted access. They must not be left unattended or in clear view when held in a location with general access.
  - Memory sticks are not permitted to be used. Schools must liaise with their IT Hub Manager if exceptional circumstances require them to be used.
  - Staff must not use computer/ laptop hard drives (c:/drive) or the desktop to store personal information as this drive is not backed up. Use your personal drive only for information that is confidential or personal or does not need to be shared within the Trust. Use Microsoft One Drive where available to do so.
  - All electronic devices must be password-protected to protect the information on the device in case of theft.
  - All members of staff are provided with their own secure login and password which must not be divulged to anyone else.
  - All staff members should implement a clear desk policy to avoid unauthorised access to physical records containing sensitive or personal information. All confidential information will be stored in a securely locked filing cabinet, drawer or safe with restricted access.
  - Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of school containing sensitive information should be supervised at all times.
  - The physical security of the Trust’s buildings and storage systems, and access to them, is reviewed by relevant senior staff and the DPO to evaluate the risks of vandalism, burglary or theft, safeguarding risk or data security and provide guidance on measures to reduce risk accordingly.

## Data Breaches

- The Trust takes seriously any data breach and will, through its policy and practice endeavour to minimise the risk of a breach. However, in the rare circumstances surrounding a data breach a process will be followed.
- The DPA states that breaches should be referred to the Information Commissioners Office (ICO) within 72 hours of disclosure. However, it is appropriate for our Trust to consider the following factors before referring to the ICO:



## Categories of Data Loss

- For easy identification and analysis of data incidents we will use the following categories internally:

### Data Breach

- Loss of data / data incident requiring a referral to the ICO

### Data Loss

- Data loss / incident requiring referral by an academy to the DPO, but after consideration is not requiring of referral to the ICO but still constitutes internal reviews, responses and possible actions

### Data Occurrence

- A data 'event' that is not the fault of an individual academy /person, will have little impact and does not require any significant response

### Complaints

- Complaints related to the management of data in our Trust will be handled through our existing Complaints Procedure. Copies of which are available on the Trust website or from the Trust office upon request.

### Requests for Amendments of Data

- The GDPR establishes the right to amend any data held that is inaccurate or may have a negative or detrimental effect on an individual. Amendments may take the form of updates, redactions or removals. As a Trust, we believe that before any amendment request is granted the first step is to view the data so as to ensure that it may be necessary. However, in the rare circumstances surrounding a data amendment request a process will be followed. This process can be seen in Appendix B

### Transparency and Accountability

- To ensure that the Trust is open and transparent about what data it holds and how it will be managed, the Trust will bear in mind the following prompts in all that it does:



- The Trust will provide every parent with information in relation to their data rights. In addition, it will also provide every new parent with a data statement. This ‘statement’ will outline the aspects of data that the Trust will gather and use, as well as stating their purpose, their ‘shelf-life’ and where it may be shared. Parents will be asked to acknowledge their understanding of this information and accept the reasoning and processing that may occur.

### Trust Website

- The Trust will establish information on its website to ensure that its approaches, policies and practices in relation to data are transparent. It will provide parents with information that may be relevant to their data concerns.
- It will include:
  - Information about the Trust’s Data Protection Officer (name, contact details etc.)
  - Copies of relevant policies
  - Data review and amendment request forms
  - Process flowcharts
  - Step by step guides
  - Complaints policy
  - Notices of amendments or additions to parental data statements or data processing

### Introducing a New Initiative or Project : Data Protection Impact Assessments

- DPIAs’ are an essential part of our accountability obligations. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals.
- By considering the risks related to data processing in advance, it increases awareness of privacy and data protection issues within our Trust. It also ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a ‘data protection by design’ approach.
- A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate compliance with all data protection principles and obligations.
- An effective DPIA allows us to identify and fix problems at an early stage.

- It can reassure individuals that their interests are being protected.
- Conducting and publishing a DPIA can also improve transparency and make it easier for individuals to understand how and why their information is being used,
- There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on.

### **The Trust's Rights to Refuse a Request**

- The Trust reserves the right to refuse a request to view or amend data held. This would be rare and only on the following basis:
- Vexatious requests
- Where information held maybe required by future legal processes e.g. Child Protection
- The request would lead to inaccurate and misleading information being recorded
- The request has come from an individual who has no rights of access

Where the Trust decides not to adhere to a request it will notify the person who requested of:

- The reason why the request has been refused
- Their legal rights of appeal or complaint
- Their legal rights of referral to the ICO

### **Charges**

The Trust will not usually make a charge in relation to data viewing or amendment requests. However, it reserves the right to do so where the request is proven to be:

- Vexatious
- Excessive
- Unfounded

### **Generic Policies**

The Trust will undertake to review all of its policies (curriculum, safety, statutory etc.) to ensure that any potential data management issues are identified and resolved. The review statement will accompany the relevant document. This process will be undertaken as part of the current policy review cycle and all policies updated in due course.

### **Training for Staff**

- In line with the Data Protection Act 2018 requirements, all new staff should be issued with a Data Management Induction pack within one week of starting their post. They should also undergo a Data Management Induction training session in their first term.
- 
- All staff will undergo refresher Data Management Training every two years.

### **On-going Guidance and Support for Staff**

The UK GDPR requires all staff to undergo training at key points during their employment.

For Trust staff the schedule of training requirements is as follows :



- Within the Trust we use a training matrix for data management training. This identifies the key knowledge that individual roles require and recognises the specific nature of some knowledge that is required by specific roles.
- There is also a recognition that staff may well be changing roles and therefore may not require training or support in all aspects of data management OR may need additional knowledge relevant to their new role. It is for Principals or line managers to identify what specific support is required for individuals in these circumstances and to liaise with the DPO to deliver it.
- The training matrix is kept under review and is adapted to meet the changing data management needs within the Trust.

### Equality Impact Assessment

- Under the Equality Act 2010 we have a duty not to discriminate against people based on their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe it is in line with the Equality Act 2010 and it is fair, it does not prioritise or disadvantage any pupil and it helps to promote and encourage equality in our academies.

### Data Protection Statement

- The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.
- All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What?	Probable Content	Why?	Who?	Where?	When?
Data Protection Policy	Any personal information including personal sensitive information	Required to be retained as part of education , statutory process	Principal / SLT, Trust central team, staff or other representative as required as part of the relevant process	Kept on file at academy (and Trust central where appropriate).	Held on file following relevant retention periods (dependent on nature of personal information)

- As such, our assessment is that this policy:

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
		✓



## APPENDIX A – Data Protection policy checklist

The Principal confirms the following is in place for [REDACTED] Academy

	Initials (Principal)
All staff have received training within the past two years to ensure they understand their duties regarding data (obtaining, recording, holding, disclosing, destroying or otherwise using data)	
All new staff receive data protection induction training within a half term of starting their role and information as soon as they start their role.	
All staff have been made aware of the data protection principles	
Personal and sensitive data is maintained securely (online and hard copy)	
The academy has an identified Information Asset Owner	
The academy has an information asset register which is updated at least termly	
Every effort is made to ensure data is only shared appropriately and with those who have a right to it (including permissions to view online data).	
Data breaches and incidents are reported to the DPO as soon as possible	
Prior to new data being collected or it being used for a new purpose, a data protection impact assessment is completed.	
The academy website identifies: <ul style="list-style-type: none"> <li>• The name and contact details of the DPO</li> <li>• Copy of the Data protection policy</li> <li>• Copy of the complaints policy</li> <li>• Notices or amendments to data processing procedures</li> </ul>	

### Infrastructure responsibilities

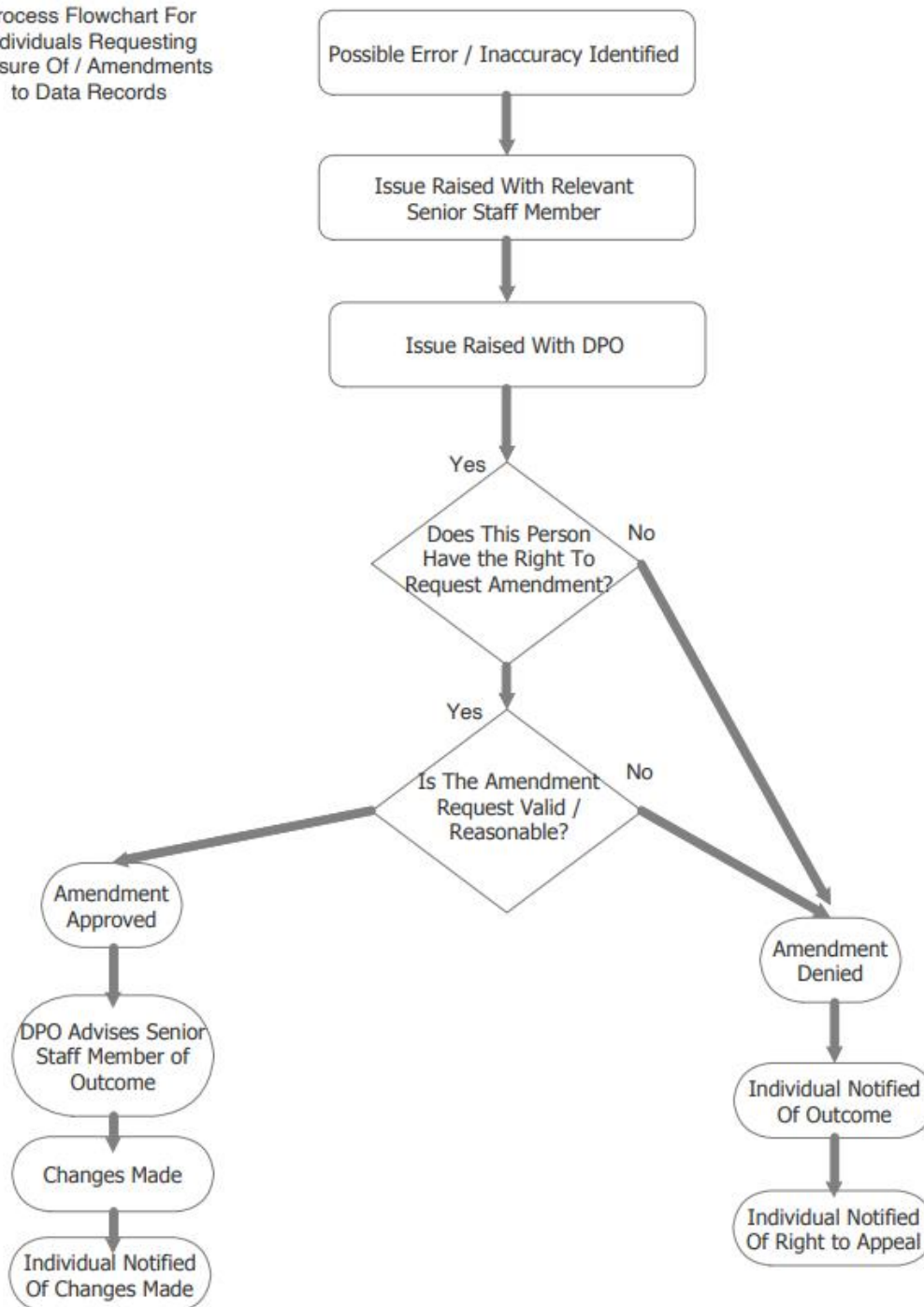
	Agreed by	Initials
HR procedures are managed in line with data protection responsibilities	Amy McColgan	
The IT system is secure and maintained in line with Trust procedures	Dave Taylor	

### Data Protection Officer

	Initials (Colin Bellis)
The DPO undertakes an audit of each academy's data arrangements at least annually and reports to the Board.	
The DPO investigates reported data breaches and incidents in line with policy	

## APPENDIX B – Flowchart for requesting erasure / amendment of data

Process Flowchart For  
Individuals Requesting  
Erasure Of / Amendments  
to Data Records



## APPENDIX C – Key Data Management Links

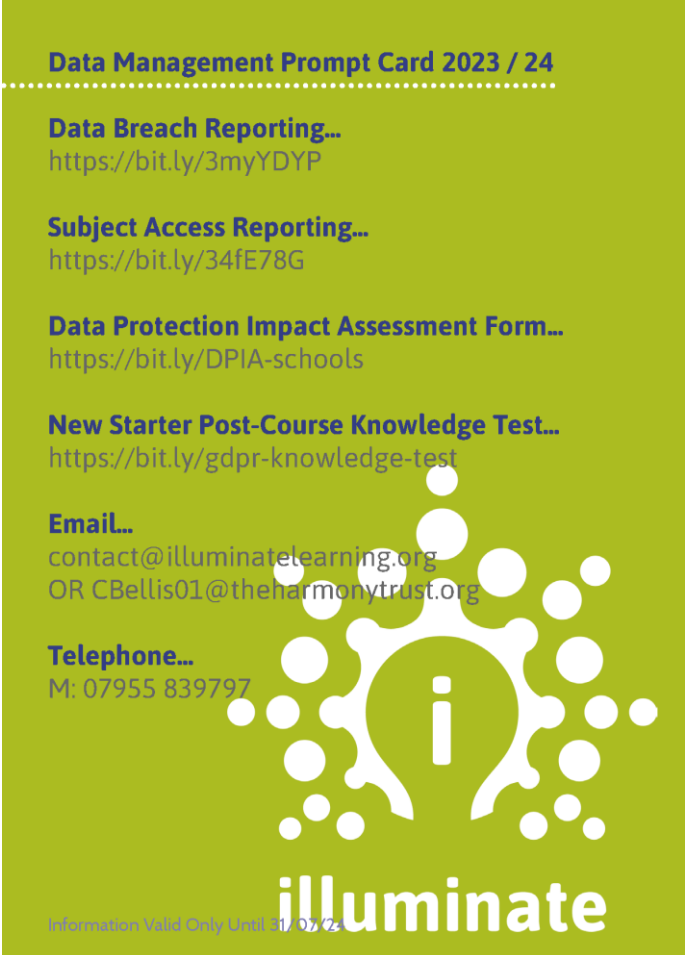
The following links should be used for specific areas of data management:

**Data Breach Reporting** ... <https://bit.ly/3myYDYP>

**Subject Access Request Reporting** ... <https://bit.ly/34fE78G>

**Data Protection Impact Assessment Form** ... <http://bit.ly/DPIA-schools>

**Essential Training Knowledge Test** ... <http://bit.ly/gdpr-knowledge-test>



**Data Management Prompt Card 2023 / 24**

**Data Breach Reporting...**  
<https://bit.ly/3myYDYP>

**Subject Access Reporting...**  
<https://bit.ly/34fE78G>

**Data Protection Impact Assessment Form...**  
<https://bit.ly/DPIA-schools>

**New Starter Post-Course Knowledge Test...**  
<https://bit.ly/gdpr-knowledge-test>

**Email...**  
contact@illuminatelearning.org  
OR CBellis01@theharmonytrust.org

**Telephone...**  
M: 07955 839797

**illuminate**

Information Valid Only Until 31/07/24

## **APPENDIX D – Further guidance to support the implementation of this policy.**

- To support the effective implementation of this policy and to meet legal obligations and requirements a Comprehensive Data Management Guide has been produced. This provides specific guidance in relation to the application of this policy. The content of this guide will be regularly reviewed in the light (a) changing legislation and (b) the analysis of issues and practice that occur within the operation of this policy.

The guide provides specific guidance on:

- Data Management Training for Staff
- Data Protection Impact Assessments
- Document Retention
- Encryption
- Using Personal Devices
- Data Safety and Security
- Subject Access Requests
- Data Breach Response Plans

To complement the comprehensive guide a variety of factsheets are produced to address specific issues that have data management issues associated with them. Staff should take notice of the advice provided within them as they provide key information. These are available via the Data Management Library on MS Teams.