

UNCONTROLLED if COPIED or PRINTED

Keswick School Multi Academy Trust is not liable for the contents of this document

DATA PROTECTION (KSMAT/STAT/023)

Committee Responsible:	Directors Keswick School Multi Academy Trust
Lead Officer:	Executive Principal and Data Protection Officer
Date of Review	March 2024
Date to be Reviewed:	March 2025
Signed:	
Date:	

DATA PROTECTION

Review Sheet

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Version Description	Date of Revision
1	Original	April 2018
2	Policy Check	March 2019
3	Policy Check and Update following data protection changes	March 2021
4	Third party updated	October 2023
5	Policy reviewed alongside Kym Allan policy v21	March 2024

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

DATA PROTECTION

Contents

1.0	Statement of Intent	Page 4
2.0	Legal Framework	Page 4
3.0	Associated Policies	Page 5
4.0	Definitions	Page 5
5.0	Compliance	Page 7
6.0	Data Protection Principles	Page 7
7.0	Accountability	Page 8
8.0	Roles and Responsibilities	Page 9
9.0	Lawful Processing	Page 10
10.0	Privacy Notices	Page 11
11.0	Consent	Page 11
12.0	The Right to be Informed	Page 12
13.0	The Right to Access	Page 12
14.0	The Right to Rectification	Page 14
15.0	The Right to Erasure	Page 15
16.0	The Right to Restrict Processing	Page 16
17.0	The Right to Data Portability	Page 17
18.0	The Right to Object	Page 17
19.0	The Right to Object to Automated Decision Making and Profiling	Page 18
20.0	Data Protection Impact Assessments	Page 18
21.0	Data Breach Notification	Page 19
22.0	Data Security	Page 19
23.0	Email	Page 22
24.0	CCTV and Photography	Page 22
25.0	DBS Data	Page 23
26.0	The Secure Transfer of Data	Page 23
27.0	Data Sharing	Page 23
28.0	Publication of Information	Page 24
29.0	Data Retention	Page 24
30.0	Data Disposal	Page 24
31.0	Training and Awareness	Page 25
32.0	Obligations to our Data Processors	Page 25
33.0	Enquiries	Page 26
	Appendix 1 - Privacy Notice: How we use Pupil Information	Page 28
	Appendix 2 - Privacy Notice: How we use School Workforce Information	Page 33
	Appendix 3 – Privacy Notice: How we use Visitor’s Information	Page 37
	Appendix 4 - Data Protection Impact Assessment (DPIA)	Page 38
	Appendix 5 - Access to Personal Data Request	Page 45
	Appendix 6 - Data Security User Checklist	Page 47
	Appendix 7 - Third party suppliers with access to Personal Data	Page 49

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

DATA PROTECTION

1.0 STATEMENT OF INTENT

- 1.1 Keswick School Multi Academy Trust (MAT) is committed to protecting the rights and privacy of individuals in accordance with its legal obligations under the Data Protection Act 2018 and the UK General Data Protection Regulations (GDPR).
- 1.2 Keswick School MAT is required to keep and process certain information about its pupils, staff and other individuals for various purposes such as:
- To support pupil learning;
 - To monitor and report on pupil progress;
 - To provide appropriate pastoral care;
 - To assess the quality of our services;
 - To ensure we operate efficiently and effectively;
 - To recruit and pay staff;
 - To collect fees;
 - To comply with legal obligations to funding bodies and the government;
 - To enable financial modelling and planning;
 - To develop a comprehensive picture of the workforce and how it is deployed.
- 1.3 Keswick School MAT may be required to share personal information about its pupils or staff with other schools, organisations, the LA and social services.
- 1.4 This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to biometric data, photographs, CCTV footage and audio and video systems.
- 1.5 This policy applies to all directors, governors, staff and volunteers who handle or have access to personal data regardless of where they are physically working e.g. home, at another organisation, on a trip and to all personal information processed by us or on our behalf. This includes the personal data accessed or used by other organisations which work for or with us e.g. local authority workers, contractors, other service providers. It may also include the personal data of other people which pupils acquire through school work tasks e.g. survey results and pupils have some responsibilities in line with their capacity to understand and follow rules.

2.0 LEGAL FRAMEWORK

- 2.1 The Data Protection Act (DPA) 2018 provides a legal framework for data protection in the United Kingdom (UK). It incorporates the General Data Protection Regulations (GDPR), the legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU) and is sometimes referred to as UK GDPR.
- 2.2 In accordance with the DPA, we at Keswick School Multi Academy Trust recognise that we collect and process personal data and because we decide how and why we do that, we are the data controller. This means that we have legal obligations regarding how we handle data and manage privacy and Keswick School MAT must be registered with the Information Commissioner's Office

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

(ICO). Anyone can read the details of our ICO notification by going online to <https://ico.org.uk/esdwebpages/search> and entering our registration number.

2.3 Data controllers are normally organisations and not people. Although the Head teacher is responsible for the day-to-day activities in school, the Trust have appointed a Data Protection Officer (DPO) be the first point of contact for data protection matters.

Our ICO Registration Number is: ZA302141

Our Data Protection Officer is: Ruth Lawler (Director of Finance & Operations)

Tel: 017687 71612

Email: ruthlawler@keswick.cumbria.sch.uk

2.4 We recognise that when we process personal data it can involve collecting, recording, organising, storing, altering, retrieving, using, disclosing, restricting and erasing or destroying it and there can be risks associated with that processing to the people whose data it is. Failure to adequately protect people's personal information can result in significant, even life-changing harm to some individuals, distress, loss of public trust in us and legal repercussions including fines and other sanctions.

2.5 The DfE provides access to a [Data Protection toolkit](#) for schools and we will make use of that toolkit as necessary.

2.6 This policy also other has due regard to other legislation, including, but not limited to the following:

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

3.0 ASSOCIATED POLICIES

3.1 This policy should be read in conjunction with the following policies and procedures:

- Safeguarding Statement (KSMAT/STAT/106)
- Child Protection and Safeguarding (KSMAT/STAT/040)
- Online Safety (KSMAT/STAT/034)
- CCTV (KS/F&P/093)
- Freedom of Information (KSMAT/STAT/068)
- Health & Safety Parts 1,2,& 3 (KSMAT/STAT/046)
- Use of Names and Images (Photography and Videos) (KSMAT/STAT/045)
- Data Security Breach Management (KSMAT/STAT/052)
- MAT Financial Regulations: ICT Security policy (KSMAT/STAT/001/APP7)
- Records Management policy (KSMAT/STAT/020)
- Staff Code of Conduct (KSMAT/STAT/039)
- Behaviour (KSMAT/STAT/044)

4.0 DEFINITIONS

4.1 '**Personal data**' refers to any information that relates to an identifiable, living person ('data subject') which identifies them. This could include information such as name, address, email address, telephone numbers, photographs, expressions of opinion about an individual, or an

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

online identifier (for example an IP address or roll number). Some of this category of personal data will require enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls e.g., a locked filing cabinet. This will be determined on the basis of a risk assessment of the harm that failing to secure the data might cause e.g. bank details due to the risk of potential fraud, contact information due to potential harassment, etc.

- 4.2 **‘Special categories of personal data’** includes biometric data, disability status, sexual orientation, ethnicity, medical information (both physical and mental health), political, philosophical and religious beliefs, trade union membership and actual or alleged criminal activities. This category of personal data requires enhanced security measures such as encryption, password protection and stricter electronic as well as manual access controls.
- 4.3 **‘Data Controller’** refers to any individual or organisation who controls personal data, in this instance Keswick School MAT.
- 4.4 **‘Data Processor’** are third party organisations which process data on our behalf. They make no decisions about how and why they do that, they just do what we ask them to within the terms of our contract.
- 4.5 **‘Processing’** refers to any operation which is performed on personal data such as: collection, recording, organisation, storage, alteration, retrieval, use, disclosure, dissemination or otherwise making available, combination, restriction, erasure or destruction.
- 4.6 **‘Data Subject’** refers to an individual who is the subject of the personal data, for example:
- Employees (current and former) and their emergency contacts/next of kin,
 - Pupils (including former pupils) and their emergency contacts/next of kin,
 - Recruitment applicants (successful and unsuccessful),
 - Agency and other partner organisation workers e.g. supply or peripatetic teachers, educational psychologists (current and former),
 - Casual workers (current and former),
 - Contract workers (current and former),
 - Volunteers (including members, directors and governors) and those on work placements,
 - Claimants.
- 4.7 **‘Pseudonymised personal or sensitive personal data’** is information that has been de-personalised but key-coded and it can fall within the scope of the UK GDPR and this policy depending on how difficult it is to attribute the pseudonym to a particular individual.
- 4.8 **‘Supervisory Authority’** is the body that regulates compliance with the GDPR and in the UK this is the ICO.
- 4.9 **‘Third country’** is the designation given to a country where there is no privacy and security of data equivalence agreement and transfers of personal data are restricted unless the data is specially protected, or an exception applies. The UK is a ‘third country’ to states in the EU GDPR zone (the EU member states plus Norway, Liechtenstein and Iceland) so, the exceptions that apply to the UK are the [adequacy decision on transfers under EU GDPR](#) and the [adequacy decision on transfers under the Law Enforcement Directive](#) on data transfers between the EU and UK. A ‘third country’ to the UK, is any state or country worldwide which is not a part of the UK and to which the UK under UK GDPR restricts transfers of personal data unless the personal

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

data is specially protected, or an exception applies. The exceptions that apply to some of these ‘third countries’ are limited and described in the [adequacy decisions](#) the UK has made.

5.0 COMPLIANCE

- 5.1 Compliance with this policy is the responsibility of all the members of Keswick School MAT who process personal data (including directors and governors).
- 5.2 Any breach of this policy, or of the Regulation itself must be reported to our Data Protection Officer and may need to be reported to the ICO as the Supervising Authority for the United Kingdom. The breach could be unlawful and result in legal action or prosecution and regardless of any legal repercussions it may also be actionable under our disciplinary procedures. A serious or deliberate breach could lead to dismissal.
- 5.3 Personal information will only be shared where it is lawful to do so and third parties must agree to abide by this policy and comply with the principles of the DPA (2018) and UK GDPR.
- 5.4 This policy will be updated, as necessary, to reflect best practice in data management, security and control and to ensure compliance with any change or amendment to the DPA (2018), UK GDPR and any other relevant legislation.

6.0 DATA PROTECTION PRINCIPLES

6.1 We will make anyone with whom we share the personal data of our data subjects aware of our relevant policy, procedures and expectations at the outset of sharing.

6.2 In accordance with Article 5 of the DPA (2018), personal data will be:

a) Processed lawfully, fairly and in a transparent manner.

We aim to achieve this through carefully considering why we need data before we ask people for it; by publishing our Privacy Notices, implementing them and reminding people about what the notices say when we ask for data; and by educating our workforce on what they mean for their day-to-day practice.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

By keeping our Privacy Notices updated, implementing them and educating our workforce about what we have and have not agreed to use data for, we can ensure we meet this obligation to restrict our processing of personal data. The law does allow us to further process data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notice.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

We will not seek to collect or process personal data which is not strictly necessary for the reasons we asked to be given it. We keep this in mind when we draft data requests and when irrelevant information is provided, we take all reasonable steps to return or erase it.

d) Accurate and, where necessary, kept up-to-date; ensuring that inaccurate personal data is erased or rectified without delay.

We review and update personal data on a regular basis. It is the responsibility of individuals providing personal data to ensure it is accurate. Individuals should notify us by any reasonable

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

means, but preferably in writing, if their personal data needs to be updated e.g., a change of name or contact details. We will take every reasonable step to ensure that inaccurate personal data (after considering the reasons it is being processed), is erased or rectified without delay. Some records are historical and should not be changed.

e) Kept in a form which permits identification of individuals for no longer than is necessary.

We follow strict information transfer guidelines when we need to move data e.g., when a pupil leaves to attend another school. We hold reviews of the data we retain and destroy or archive in line with guidance from [IRMS Academies Toolkit - Information and Records Management Society](#).

The law does allow us to retain personal data for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes and we have declared that we might do this in our Privacy Notices.

f) Processed in a manner that ensures appropriate security of it.

We understand that our organisational and technical measures to protect data must include protection against unauthorised or unlawful processing and against accidental loss, destruction or damage in the UK, European Union or anywhere else in the world.

We make staff and volunteers aware of their data protection responsibilities and that their duty to preserve confidentiality extends to anywhere that they process the data of our data subjects e.g. at home, on trips etc. and beyond their time of employment with us.

7.0 ACCOUNTABILITY

7.1 Keswick School MAT is the registered Data Controller with the Information Commissioner’s Office (ICO) and is responsible for controlling the use and processing the personal data it has collected.

7.2 Keswick School MAT will implement technical and organisational measures to demonstrate that data is being processed in line with the principles set out in this policy. This will include:

- Providing comprehensive, clear and transparent privacy notices (Appendix 1 and 2).
- Using data protection impact assessments (DPIA), where appropriate (Appendix 3).
- Recording activities relating to higher risk processing, such as the processing of special categories of personal data.

7.3 The privacy notices (Appendix 1 and 2) explain how Keswick School MAT will share personal data with third parties. This will only occur following consent from the Data Protection Officer (DPO). The sharing of personal data is generally limited to enabling the MAT school to perform its statutory duties or in respect to a child's health, safety and welfare.

7.4 Internal records of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

7.5 Individuals who provide personal data to Keswick School MAT are responsible for ensuring that the information is accurate and up-to-date.

8.0 ROLES AND RESPONSIBILITIES

8.1 Our responsibilities as a data controller include:

- Analysing and documenting the types of personal data we hold and their uses.
- Identifying our lawful basis for processing personal data.
- Having procedures which support the rights of the individual.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing risks to individual rights and freedoms should data be compromised.

8.2 Staff responsibilities include:

- Understanding their data protection obligations in line with their training and professional duties and Raising concerns, notifying breaches or errors and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.
- with our relevant policies and procedures e.g. the Online Safety Policy when remote working, etc.
- Checking that their data processing activities comply with our policies and are justified.
- Not using data in any unlawful way.
- Storing data carefully and correctly to avoid breaches of data protection.

8.3 The Data Protection Officer's responsibilities include:

- Keeping governors/trustees updated about data protection responsibilities, risks and issues.
- Reviewing the data protection policy, associated policies and all relevant procedures regularly.
- Arranging data protection training and advice for all staff and others included in this policy.
- Advising on direct marketing issues such as compliance with the law and our policy; how we deal with queries from target audiences or media outlets; and the wording of data protection statements attached to emails and other marketing copy.
- Answering questions on data protection from staff, governors/trustees and other stakeholders.
- Responding to individuals such as parents, pupils and employees who want information.
- Checking on and approving of any third parties that handle our data and any contracts or agreements regarding data processing.

8.4 The ICT Network Manager's responsibilities include:

- Ensuring all systems, services, software and equipment meet acceptable security standards and can be appropriately filtered and monitored.
- Checking security hardware and software regularly to ensure it is functioning properly and securely.
- Researching relevant third-party services (cloud services, data shredding etc.) that we are considering using.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

9.0 CONDITIONS FOR LAWFUL PROCESSING

- 9.1 Personal data can be lawfully processed under the following conditions:
- Consent of the data subject.
 - Compliance with a legal obligation.
 - Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
 - 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.
 - Necessary for legitimate interests of the controller or third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.
- 9.2 To process the personal data of our workforce and volunteers, we generally rely on (d). However, some pieces of data are processed for other reasons, i.e. we use National Insurance numbers for tax purposes (b), next of kin details in an emergency (e), images for ID badges (f).
- 9.3 To process the personal data of pupils we generally rely on (c), to educate them. Some pieces of data are processed for other reasons, i.e. we publish results relying on (b) because the law requires us to, we hold next of kin data (e).
- 9.4 We rely on different conditions to process different pieces of the personal data of families, e.g. (d) for financial details to provide school meals and (e) for contact details in case a student is ill.
- 9.5 Special categories of personal data can be lawfully processed under the following conditions **as well as** one condition in the table above:
- Explicit consent of the data subject, unless prohibited by EU/National 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 already made public by the data subject.
 - 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 person 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 EU/National 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 EU/National law or a contract with a health professional.
 - Reasons of public interest in the area of public health e.g. protecting against serious cross-border threats to health or ensuring high standards of healthcare & medicinal products or medical devices.
- 9.6 We rely on different conditions for the lawful processing of sensitive personal data for different things, i.e. (d) to check criminal history before employing individuals, (d) for child protection and

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

multi-agency safeguarding work regarding pupils, (d) or (h) to use health information to protect pupils at school.

9.7 More than one lawful basis may apply, but we only need **one** basis for each piece of data and we will rely on what best fits the purpose, not what is easiest. When carrying out a new task or an existing task in a new way, staff should consider the following factors:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are we in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are we able to stop the processing at any time on request and have we factored in how to do this?

10.0 PRIVACY NOTICES

10.1 Our Privacy Notices are an important and necessary way of being transparent and telling governors/ trustees, parents, pupils, staff, contractors and visitors what we are doing with their information. To comply with the law, it will include:

- Our identity and contact details as the data controller and those of our DPO.
- The purpose of the processing and the lawful basis or bases we are relying on.
- Our, or a third party's legitimate interests in having it.
- The categories of personal data we process.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to UK Government determined "third countries" and the safeguards.
- Retention periods or the criteria used to determine them.
- The existence of each of the data subject's rights.
- The right to withdraw consent at any time, where relevant.
- The right to lodge a complaint with the ICO.
- The sources of personal data and whether they are publicly accessible.
- Whether providing personal data is statutory or contractual and the possible consequences of failing to provide it.
- The existence of any automated decision making, including profiling; how decisions are made, the significance and the consequences.

See the Contents Page for links to our privacy notices relevant to pupils and our workforce. These are also made available on our website and in communications with parents and staff, etc.

11.0 CONSENT

11.1 It is not always necessary to gain consent before processing personal data (see paragraphs 9.1, 9.2 and 9.3) but when it is, consent must be a positive indication.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- 11.2 When we do need consent and we ask for it, we will include the following information in our request:
- the name of our school
 - the name of any third-party controllers who will rely on the consent
 - why we want the data
 - what we will do with it
 - that individuals can withdraw consent at any time
- 11.3 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.
- 11.4 Any forms used to gather personal data will be provided with a privacy notice (Appendix 1 and 2) and will indicate whether or not the individual needs to give consent for the processing.
- 11.5 A record will be kept documenting how and when consent was given.
- 11.6 If an individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then Keswick School MAT will ensure that the processing of that data does not take place.
- 11.7 Consent can be withdrawn by the individual at any time.
- 11.8 Parental consent will be sought prior to the processing of a child's data which would require consent until the age of 16, except where the processing is related to preventative or counselling services offered directly to a child.
- 11.9 Consent will be sought from the child after the age of 16 if we consider they have the competence to consent for themselves (often referred to as the Gillick competence test). If there is any doubt parental consent will continue to be required.

12.0 THE RIGHT TO BE INFORMED

- 12.1 Our Privacy Notices seek to provide transparency about our collection of personal data; they are published on our website, pinned to noticeboards and freely available on request from our office; we draw people's attention to what they say when we collect data from them; and we regularly review and update the Notices when necessary, particularly if we have changed what we use the data for and before we start using it for the new reason.

13.0 THE RIGHT TO ACCESS

- 13.1 Individuals have the right to obtain confirmation that their personal data is being processed fairly or to submit a subject access request (SAR) to gain access to their personal data. In order to ensure individuals receive the correct information, SARs must be made in writing and submitted to the Head teacher of the school (Appendix 4).
- 13.2 The Head teacher of the school will verify the identity of the person making the request before any information is supplied.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- 13.3 We must verify the identity of the person making the request, using “reasonable means”. If the person making the request is not the data subject, we must also verify their right to make such requests on behalf of the data subject e.g., their authority to act or their parental responsibility for a child. In cases where a child is competent to make their own request, information will be provided to the child and not to the parent. We will use ICO guidance and our knowledge of the capability of our pupils as described above to make decisions about this.
- 13.4 The SAR will be recorded in the Subject Access Request log and all requests will be responded to within one month of receipt.
- 13.5 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.
- 13.6 Where a fair processing request is made the information contained within the relevant privacy notice will be provided.
- 13.7 Where a SAR is made copies of personal data will generally be encrypted and supplied to the individual in a commonly used electronic format.
- 13.8 Where a SAR is received from a pupil, Keswick School MAT’s policy is that:
- It will be processed in the same way as any other SAR. The information will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
 - Where a pupil does not appear to understand the nature of the request will be referred to their parents or carers.
- 13.9 SARs made by people on behalf of children they hold parental responsibility for will be processed in the same way as any other SAR while recognising that they do not own the data they are requesting. If we are confident that the pupil whose data it is **does** understand the SAR and their rights, then we will respond to the child rather than the parent, even where the parent was the one who made the request.
- In making our decision we will take the following, amongst other things, into account:
- the child’s level of maturity and their ability to make decisions like this.
 - the nature of the personal data.
 - any court orders relating to parental access or responsibility that may apply.
 - any duty of confidence owed to the child or young person (including information about any counselling or other service being offered directly to the child).
 - any consequences of allowing those with parental responsibility access to the child’s or young person’s information (particularly important if there have been allegations of abuse or ill treatment).
 - any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
 - any views the child or young person has on whether their parents should have access to information about them.
- 13.10 If the information requested by a parent in a SAR relates to the ‘educational record’ of a pupil, in accordance with ‘*The Education (Pupil Information) (England) Regulations 2005*’, we will make a pupil’s educational record available for inspection by the parent, free of charge, **within fifteen**

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

school days of receipt of the parent's written request for access. This cannot include any information that we could not lawfully disclose to the pupil themselves. If parents request a copy to keep, we can charge the administrative costs of supplying one.

- 13.11 If the information requested in a SAR does **not** relate to the 'educational record' of a pupil, we will provide a copy of the information free of charge **unless** the request is manifestly unfounded or excessive, particularly if it is repetitive. This fee may vary and will be based only on the administrative cost of providing the information. We will use ICO guidance and our own information management records to make decisions about this.
- 13.12 If the request is made electronically, we will provide the information in a commonly used electronic format.
- 13.13 If we are asked for a large quantity of information about an individual, we can ask the individual to be more specific about the information they want. This is not because we are exempt from providing large amounts of data, this is so we can consider whether the request is manifestly unfounded or excessive.
- 13.14 If we are asked for information that a data processor, we work with holds on our behalf, we will ask our data processor to provide it to us so that we can comply with the SAR. This is because we are the data controller and it is our responsibility. We have written contracts in place with all of our data processors to help us do this.
- 13.15 Where a request is excessive or repetitive, a 'reasonable fee' will be charged. All fees will be based on the administrative cost of providing the information.
- 13.16 Where a request is manifestly unfounded Keswick School MAT holds the right to refuse to respond to the request. The individual will be informed of this decision and the reason behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

14.0 THE RIGHT TO RECTIFICATION

- 14.1 Personal data held by Keswick School MAT will be as accurate as is reasonably possible.
- 14.2 Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where an individual informs a MAT school of inaccurate or incomplete personal data their data record will be updated as soon as is practicable.
- 14.3 Parents at Keswick School are able to check the detail we held on our school management information system by signing into Edulink. They can request amendments, and once approved by school, these automatically update our MIS. Parents at Bassenthwaite School receive a data sheet at the beginning of autumn term and again in the summer term to ensure student records are kept up to date.
- 14.4 Where the personal data has been disclosed to a third party, the MAT school will inform them of any rectification where possible. The individual will also be informed about the third parties that the data has been disclosed to where appropriate.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- 14.5 Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
- 14.6 Where no action is being taken in response to a request for rectification, Keswick School MAT 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.
- 14.7 The right to rectification will depend on why we asked for the personal data. For example: a person's name should **not** be changed to their new married name on the Single Central Record (SCR) because the SCR is a record of information correct at the time of recruitment and vetting. A note should be added to ensure the SCR record can be matched to the correct living person in case of a vetting query using the married name in future, but the record itself should not be changed.

15.0 THE RIGHT TO ERASURE

- 15.1 Individuals have the right to request erasure of personal data. This applies where:
- Personal data is no longer necessary for the purpose for which it was collected/processed.
 - Withdrawal of consent and no other legal ground applies.
 - The individual objects to the processing and there is no overriding legitimate interest.
 - Personal data is unlawfully processed.
 - Personal data has to be erased in order to comply with a law.
 - Personal data of a child is processed in relation to an online service.
- 15.2 Keswick School MAT has the right to refuse a request for erasure where personal data is being processed for:
- Exercising the right of freedom of expression and information.
 - Compliance with legal obligations or for performing tasks carried out in the public interest or in exercising the data controller's official authority.
 - Reasons of public interest in the area of public health.
 - Archiving purposes in the public interest, scientific or historical research, or statistical purposes.
 - The establishment, exercise or defence of legal claims.
- 15.3 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.
- 15.4 Where personal data has been disclosed to third parties they will be informed about the request for erasure, unless it is impossible or involves a disproportionate effort to do so.
- 15.5 Where personal data has been made public and then is requested to be erased, considering the available technology and the cost of implementation, all reasonable steps will be taken to inform other data controllers about the request for erasure.
- 15.6 When we receive a request to erase data, we will take reasonable steps to check the identity of the requester and that they have the right to make the request before considering it.
- 15.7 We can refuse to comply with a request when an exemption applies, or when the request is manifestly unfounded or excessive. We can either request a reasonable fee based on the

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

administrative costs of complying with the request, or we can refuse to deal with the request. We will use ICO guidance and our own information management records to make decisions about this and we will contact the person making the request to inform them of our decision (including any fee payable) and the reasons without undue delay and **within one month**. We do not have to comply with the request until we have received the fee.

15.8 When we have decided whether we can erase the data we will explain our decision to the individual making the request and inform them of their rights to complain to the ICO. We will also make a record of the request and our response similar to the way we handle SARs e.g., date and manner of request (verbally to class teacher, a note handed to reception etc.), the data subject's name, the name and address of requester (*if different*), the erasure requested, our decision and the date we communicated the decision.

16.0 THE RIGHT TO RESTRICT PROCESSING

16.1 Individuals have the right to restrict the school's processing of personal data.

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

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

- a) Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data.
- b) Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual.
- c) Where processing is unlawful and the individual opposes erasure and requests restriction instead.
- d) Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

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

16.5 We use the most appropriate method applicable at the time to restrict processing including:

- temporarily moving the data to another processing system.
- making the data unavailable to users; or
- temporarily removing published data from a website.

16.6 While a restriction is in place, we will not do anything with data except store it unless:

- we have the individual's consent.
- it is for the establishment, exercise, or defence of legal claims.
- it is for the protection of the rights of another person; or
- it is for reasons of important public interest.

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

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

17.0 THE RIGHT TO DATA PORTABILITY

- 17.1 Individuals have the right to obtain and reuse their personal data for their own purposes across different services.
- 17.2 Personal data can be moved, copied or transferred from one IT system to another in a safe and secure manner, without hindrance to usability.
- 17.3 The right to data portability only applies when all 3 of the following conditions are met:
- a) the individual has provided the personal data;
 - b) the processing is based on the individual’s consent or the performance of a contract; **and**
 - c) processing is carried out by automated means.
- 17.4 Keswick School MAT will respond to any requests for portability within one month and will provide the personal data free of charge and in a structured and commonly used form.
- 17.5 Where feasible, data will be transmitted directly to another organisation at the request of the individual. Keswick School MAT is not required to adopt or maintain processing systems which are technically compatible with other organisations.
- 17.6 In the event that the personal data concerns more than one individual, Keswick School MAT will consider whether providing the information would prejudice the rights of any other individual.
- 17.7 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 receipt of the request.
- 17.8 Where no action is being taken in response to a request Keswick School MAT will, without delay and at the latest within one month, explain the reason for this. The individual will also be informed of their right to complain to the supervisory authority and to a judicial remedy.

18.0 THE RIGHT TO OBJECT

- 18.1 Individuals must have an objection on “grounds relating to his or her particular situation” and we must stop processing the personal data unless:
- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
 - the processing is for the establishment, exercise, or defence of legal claims.
- 18.2 We will:
- inform individuals of their right to object “at the point of first communication” and in our privacy notices, explicitly bringing the right to their attention clearly and separately from any other information.
 - stop processing personal data for *direct marketing purposes* as soon as we receive an objection because there are no exemptions or grounds to refuse; and
 - deal with an objection to processing for *direct marketing* at any time and free of charge.
- 18.3 An individual can object to processing for research purposes on “grounds relating to his or her particular situation” unless processing is necessary for the performance of a public interest task.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

18.4 We carry out some processing of personal data securely in encrypted online systems e.g. our visits approval system, responding to DfE data demands online and any individual can object to our online processing by contacting the Headteacher.

19.0 THE RIGHT TO OBJECT TO AUTOMATED DECISION MAKING AND PROFILING

19.1 We do not currently use any data systems that make automatic decisions about people without any human involvement. We are aware of our legal obligations and will follow [ICO guidance](#), reviewing our policy and procedures if we fully automate any decision-making.

20.0 DATA PROTECTION IMPACT ASSESSMENTS

20.1 Keswick School MAT will act in accordance with the DPA (2018) by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how the MAT has considered and integrated data protection into processing activities.

20.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with data protection obligations and meeting individuals' expectations of privacy (Appendix 3).

20.3 DPIAs will allow Keswick School MAT to identify and resolve problems at an early stage, thus preventing reputational damage which might otherwise occur.

20.4 All DPIAs will 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.

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

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

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

- Systematic and extensive processing activities.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

20.8 Where a DPIA indicates high risk data processing, Keswick School MAT will consult the ICO to seek its opinion as to whether the processing operation complies with the DPA (2018).

20.9 The need for a DPIA should be reported to the DPO who will work with other members of staff to complete it.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

21.0 DATA BREACH NOTIFICATION

- 21.1 The term 'data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- 21.2 Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed. A qualifying data breach is one where, if not addressed in an appropriate and timely manner, it could result in physical, material or non-material damage to someone such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to them.
- 21.3 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of Keswick School MAT becoming aware of it.
- 21.4 The risk of the breach having a detrimental effect on the individual and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.
- 21.5 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, Keswick School MAT will notify those concerned directly.
- 21.6 In the event that a breach is sufficiently serious, the public will be notified without undue delay.
- 21.7 Effective and robust breach detection, investigation and internal reporting procedures are in place, which will guide decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
- 21.8 Within a breach notification, the following information will be outlined:
- The nature of the personal data breach, including categories, approximate number of individuals and records concerned.
 - The name and contact details of the DPO.
 - 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.
- 21.9 Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures may be liable to disciplinary action. Where others have been involved in a data breach, a report will also be made to their employer or DPO if relevant to the breach.

22.0 DATA SECURITY

- 22.1 Keswick School MAT undertakes to ensure the security of the personal data it has collected. Personal data will only be accessible to those who have a valid reason for using it.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

22.2 All the members of Keswick School MAT (including directors and governors) are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party (a data security user checklist is provided for quick reference in Appendix 5).

22.3 **Physical measures**

- a) Premises security measures, such as alarms, safes, deadlocks, are in place.
- b) Only authorised persons are allowed in the IT office.
- c) Data storage devices and printouts are locked away securely when not in use.
- d) Visitors to MAT schools are required to sign in and out, wear identification badges and are, where appropriate, accompanied.
- e) Premises security and storage systems is reviewed on a regular basis. If an increased risk in vandalism/theft is identified, extra measures to secure data storage will be put in place.

22.4 **Technical measures**

- a) Security software is installed on MAT school networks and electronic devices. This includes:
 - Internet filtering and firewall
 - Anti-virus
 - Email ransom ware detection
- b) Data on MAT school network drives is password protected and automatically backed up off-site. There are procedures in place to access and restore all the data held on the MAT school network drives should this be necessary.
- c) Keswick School MAT electronic devices are password protected and, where possible, have been enabled to allow remote blocking or deletion of personal data in the case of theft.
- d) MAT users are given a secure user name and password to access the MAT school networks, Google Drive and any other learning platform they require access to.
- e) Password rules have been implemented.
- f) MAT users will be assigned a clearance that will determine which files are accessible to them. Protected files are not accessible to unauthorised users.
- g) Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
 - The device **must** be checked by an IT Technician before use;
 - It **must** be password protected;
 - It **must** be stored in a secure and safe place when not in use;
 - It **must not** be accessed by other users (e.g. family members) when out of a MAT school.
 - Personal data **must** be securely deleted when no longer required.
- h) Data breach detection tests will be undertaken to evaluate Keswick School MAT's technical measures and minimise the chance of a data breach.

22.5 **Organisational measures**

- a) Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.
- b) Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).
- c) Paper records containing personal data **must** be kept secure if they are taken off the school premises.
- d) MAT users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically (Online Safety Policy - KSMAT/STAT/034).

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- e) Passwords **must** be alphanumeric, including one capital and one special character and be a minimum of 8 characters long to access the school network and Google Drive.
- f) MAT user names and passwords **must not** be shared.
- g) MAT electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.
- h) Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.
- i) Emails **must** be encrypted if they contain personal data and are being sent outside the UK (boarding pupils).
- j) Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
- k) Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- l) Visitors to MAT school premises containing special categories of personal data **must** be supervised at all times.
- m) Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
- n) Personal data **must not** be disclosed to any unauthorised third parties.
- o) Personal electronic devices **must not** be used to hold personal data belonging to Keswick School MAT.
- p) Personal electronic devices **must** be password protected and have up-to-date, active anti-virus and anti-malware checking software before being used to access personal data belonging to Keswick School MAT via:
 - A password protected removable storage device;
 - The remote desktop protocol (i.e. remote access to the school network);
 - Google Drive (including Google docs, Google classroom etc).
- q) Personal electronic devices that have been set to automatically log into the school network, school email accounts or Google drive that are lost or stolen **must** be reported to the DPO so that access to these systems can be reset.
- r) Google file stream can be used but copies of documents containing personal data **must not** be stored as local copies on the personal electronic device.
- s) If personal data is taken off Keswick School MAT premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.
- t) Before sharing personal data, Keswick School MAT staff/Governors/Directors **must** ensure:
 - They are allowed to share it;
 - That adequate security is in place to protect it;
 - Who will receive the personal data has been outlined in a privacy notice.
- u) Any personal data archived on disks **must** be kept securely in a lockable cabinet.
- v) Access to personal data in the School's Management Information System is limited by access rights. Access rights are reviewed on an annual basis or when job roles change.
- w) Pupils/staff personal paper files are stored in secure locked cupboards. Access is restricted to the Pastoral team, HR Officer and Headteacher.
- x) Keswick School MAT staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the DPA (2018).

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

23.0 EMAIL

23.1 All staff are expected to adhere to the good practice around the use of email set out in the current Information and Records Management Society '[Academies Toolkit](#)' understanding their role and responsibilities with regard to:

- the 8 things they must know about email including that it is not always a secure medium to send confidential information by, that email is disclosable under the Freedom of Information Act 2000, that any employer has a right to monitor the use of email under the Regulation of Investigatory Powers Act 2000 and that email is one of the most common causes of stress in the workplace
- creating and sending email
- sending attachments
- using disclaimers
- managing received e-mails; and
- retaining emails

23.2 All staff are required to use the authorised email disclaimer as follows:

Under the Data Protection Act 2018 and UK General Data Protection Regulation (GDPR), we have a legal duty to protect any information we collect from you. Information contained in this email and any attachments may be privileged or confidential and intended for the exclusive use of the original recipient. If you have received this email by mistake, please advise the sender immediately and delete the email, including emptying your deleted email box.

24.0 CCTV AND PHOTOGRAPHY

24.1 Keswick School MAT understands that recording images of identifiable individuals constitutes as processing personal data and so is done in compliance with DPA (2018) principles.

24.2 CCTV systems operate on MAT school premises for the purpose of protecting school members and property.

24.3 Pupils, staff, parents and visitors are notified of the purpose of collecting CCTV images via signage around the school premises.

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

24.5 CCTV footage is kept for one month for security purposes unless it is relevant to an investigation in which case it will be kept for a maximum of six months. Detailed guidance is given in Keswick School's CCTV policy (KS/FIN&PREM/093).

24.6 Keswick School MAT may occasionally use photographs/videos of pupils in a publication, such as the school website, prospectus, press release, or record a school play.

24.7 Prior to the publication of any photograph or video of pupils in the press, social media, school website and prospectus or in any other marketing or promotional materials, written consent will be sought from parents. Detailed guidance is given in the Photography and Videos at School policy (KSMAT/STAT/045).

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- 24.8 Photographs or videos captured by other individuals for recreational or personal purposes, such as pupils taking photos on a school trip or parents taking photos at prize giving, are exempt from the DPA (2018).
- 24.9 We *do not* need parental consent to process any personal data including image or voice recordings made for the purposes of education e.g. video of a Performance Assessment for a GCSE examination in PE in a sport or activity where live moderation is not possible by the school or other Assessment Centre.
- 24.10 Photography, audio recording or filming will only take place at school or school events with the permission of the Head teacher/ manager and under appropriate supervision.

25.0 DBS DATA

- 25.1 DBS information is treated as a special category of personal data under this policy.
- 25.2 DBS information will never be duplicated and any third parties who have lawful access to DBS information will be made aware of their DPA (2018) responsibilities.

26.0 THE SECURE TRANSFER OF DATA

- 26.1 Keswick School MAT is required to share personal information with the Department for Education (DfE), Education and Skills Funding Agency (ESFA), Cumberland Council, Westmorland Council, Ofsted, schools and educational institutions, public services and other third-party providers. These are outlined in the privacy notices (Appendix 1 and 2).
- 26.2 Keswick School MAT users must not remove, copy or share any personal data with a third party without permission from the DPO.
- 26.3 Where personal data is required to be lawfully shared with a third party it must be securely transferred either through a portal or be sent following encryption, using approved encryption software and be password protected.
- 26.4 No personal data will be transferred to a country outside the UK without the explicit consent from the individual. Advice must be taken from the DPO.
- 26.5 Transfers of personal data outside the UK are treated differently depending on which countries it is being transferred between or through, what is being transferred, why and how and how closely those countries' approaches to data protection align with the UK's. We will follow current ICO guidance on [International transfers after the UK exit from the EU Implementation Period](#) and [Standard Contractual Clauses \(SCCs\) after the transition period ends](#) for country specific requirements when we need to transfer personal data internationally.

27.0 DATA SHARING

- 27.1 We are required to share personal data with some organisations by law e.g. our census data with the DfE. At other times we share information to improve or protect people's lives and we have included information about this in our Privacy Notices.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

27.2 All staff are signposted to the current ICO [Data Sharing Checklist](#) in making decisions on whether to share data or not and how to do it. Unless the data sharing is routine and pre-authorised e.g. medical data routinely disclosed to the outdoor adventure centres we go on residential trips to, no decision should be made regarding the disclosure of any sensitive personal or sensitive commercial data without reference to an immediate line manager or the Head teacher. If nobody involved in the decision-making has received suitable training in data protection, the DPO must be consulted before data is disclosed externally.

28.0 PUBLICATION OF INFORMATION

28.1 A publication scheme can be found in the Freedom of Information policy (KSMAT/STAT/068) and on MAT school websites. This specifies the classes of information that will be made available on request, including:

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

28.2 Keswick School MAT will not publish any personal data on MAT school websites without consent from the affected individual(s).

29.0 DATA RETENTION

29.1 Personal data will not be kept for longer than is necessary. We will generally follow the guidelines set out in the current Information and Records Management Society '[Academies Toolkit](#)' and requirements placed on us by the Local Authority and Local Children's Safeguarding Partnership.

29.2 The DPO will ensure that obsolete personal data is properly erased. The length of time we hold personal data is set out in our Records Management policy (KSMAT/STAT/020).

29.3 Personal data that is not required will be deleted as soon as practicable.

29.4 Some educational records relating to former pupils or employees may be kept for an extended period for legal reasons, the provision of references or for historical archives.

30.0 DATA DISPOSAL

30.1 Keswick School MAT will comply with the requirements for the safe destruction and deletion of personal data when it is no longer required.

30.2 Paper documents containing personal data will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.

30.3 Hard drives of redundant PCs and storage devices containing personal data will be securely wiped clean before disposal, or if that is not possible, physically destroyed.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

31.0 TRAINING AND AWARENESS

- 31.1 During their induction, all staff and volunteers will receive suitable training in their responsibilities for data protection in their work or volunteering and the relevant procedures. This will be supplemented with staff briefings, inset training and other methods of updating staff and volunteers as necessary e.g. briefing emails, notices etc.
- 31.2 This policy is available to all staff and volunteers in digital format on the staff network (Shared Google Drive/ Current Approved Policies). A hard copy can also be obtained from the Clerk to the Governors, Annabel Scott if required. This policy will be updated regularly in line with changes in practice or clarifications required after applying it to resolve data protection issues.
- 31.3 Anyone can seek general data handling guidance from the ICO on their website <https://ico.org.uk>.
- 31.4 Day-to-day support and guidance for staff is available from:
Ruth Lawler, Data Protection Officer
Tel: 01768771612
Email: ruthlawler@keswick.cumbria.sch.uk

32.0 OBLIGATIONS TO OUR DATA PROCESSORS

- 32.1 As the data controller we have obligations to our data processors when we give them the personal data of our data subjects which include in general, but are not limited to responsibilities to:
- provide accurate personal data and all necessary corrections in a timely manner.
 - employ appropriate technical and organisational security measures when providing and using the personal data being processed.
 - only request user access to the data processing for employees and the contractor at a level commensurate with their work tasks and responsibilities e.g. have the fewest possible users who are authorised and enabled to access the accident and incident reporting system which contains sensitive health data.
 - respond promptly to requests from our processors for data updates and provide updated and accurate written instruction regarding the continued access to data that we require.
 - require our users of any data processor's system to comply with strict password security measures e.g. length, complexity, not shared etc.
 - take appropriate action regarding any breaches.
 - ensure our users of a processor's system website understand their responsibilities with regard to the DPA and the GDPR. Anyone found to have carried out unauthorised or unlawful processing activities must be made aware that they will be subject to disciplinary action by you and may be further subject to legal action or prosecution.
 - inform our processor as immediately as possible if:
 - we need to remove security access i.e. to our data on their system, from individuals who no longer have any legal right or authority to access it e.g. employees who have left our employment,
 - we need their assistance to comply with a Subject Access Request,
 - we need them to stop processing the personal data of any of our data subjects,
 - be sure of our grounds under the law for asking a processor to stop processing the personal data of any of our data subjects and that they are compatible with other applicable laws or legal rights,

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- be very sure of our grounds to erase data under the law because we can expect to pay the full costs of any extraordinary measures required to recover erased data where we have failed in our duties.

32.2 All staff involved in using the data that we control with the processing services that we contract with have a duty to meet all of our conditions of service.

33.0 ENQUIRIES

33.1 Any further information, questions or concerns about this policy or the security of data held by Keswick School MAT should be directed to the DPO (or to the Head teacher of the MAT school):
Mrs Ruth Lawler, Data Protection Officer
017687 72605

33.2 General information about the DPA (2018) can be obtained from the Information Commissioner's Office <http://www.ico.gov.uk/>.

33.3 This policy will be reviewed annually and may be supplemented by additional procedures.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Privacy Notice: How we use Pupil Information

Keswick School Multi Academy Trust is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of pupil information that we collect, process, hold and share include:

- Personal information (such as name, unique pupil number, contact details and address);
- Characteristics (such as ethnicity, language and free school meal eligibility);
- Biometric data to facilitate school access systems;
- Safeguarding information (such as court orders and professional involvement);
- Assessment information (such as reports, feedback, test data and exam results);
- Medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements);
- Attendance (such as sessions attended, number of absences, reasons for absence and any previous schools attended);
- Special Educational Needs information (such as Education and Health Care Plans (EHCPs), Individual Education Plans (IEPs) and notes from review meetings and professional assessments);
- Behavioural information (such as exclusions and any relevant alternative provision put in place);
- Post 16 learning information and destination data;
- CCTV recordings to protect the safety and security of children, staff and the school site;
- Images and voice recordings for assessment, celebration and in CCTV for safety and security reasons.
- Financial information like entitlement to meals, transport and premium funding to manage catering, school trips, etc.

Why we collect and use this information

We collect and use the pupil information, for the following purposes:

- To support pupil learning;
- To monitor and report on pupil attainment and progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To keep children and staff safe;
- To meet statutory duties placed upon us for DfE data collections;
- To celebrate or promote school, for scientific interest, or to record our own school history;
- To control access to school buildings.

The lawful basis on which we use this information

Under UK GDPR, the lawful bases we rely on for processing personal information about pupils are:

- to perform a public task i.e. to provide education
- to protect vital interests (and sometimes carry out a contract too) e.g. to provide **safe** meals, trips, transport, uniform, professional photos, childcare
- to comply with the law e.g. recording attendance, publishing results, recording the census (see Sharing with the DfE below), data sharing with child protection partners like social care, the NHS, and the Local Authority etc. (see sharing with the DfE below for legislation).
- having consent e.g. use images or names publicly.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

When we process special category data like medical information or biometrics, we need to have one lawful basis from the list above *and one* of the following list:

- to prevent medical problems, assess needs, and provide services e.g. Education Health & Care Plans (EHCP), records of medicines administration.
- to improve public health e.g. report notifiable diseases to local and national government departments;
- to make or defend legal claims e.g. some special educational needs and all accident records.
- having consent e.g. to use biometric data to access school buildings.

How we collect pupil information

We collect pupil information from parent/guardians at the start of the school year, Common Transfer File (CTF) and secure file transfer from previous schools.

Most of the pupil information we ask for is required by law or necessary so we can provide a good education and some of it is voluntary. To comply with UK GDPR, if you have a choice about providing information, we will tell you when we ask for it. We will also tell you what to do if you do not want to share this information with us.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our Records Management Policy (KSMAT/STAT/020). For more information on data retention and how we keep your data safe, please see our Data Protection policy (KSMAT/STAT/023) which can be downloaded from our website.

Who we share pupil information with

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like School to School, via a contractor's secure data sharing system like our online school trips safety system, and sometimes in other secure ways.

We routinely share pupil information with:

- Other parts of our MAT to monitor the quality of our provision, benchmark locally, and to make decisions about local policy, practice and funding.
- Schools and other education providers pupils go to after leaving us to support their continuing education;
- Child development and protection partners like our local Authority Children's Services, Public Health, Inclusion & Social Care etc. to check attendance, monitor, and protect children; the NHS for medical referrals & support; private companies offering counselling and other family or support services.
- The DfE to help decide our school funding, monitor attainment and benchmark it nationally, compile league tables, develop national education policy and monitor it.
- Our Local Authority to ensure they can conduct their statutory duties such as under the [Schools Admission Code](#), including conducting Fair Access Panels, and careers guidance legislation.
- Medical services like therapists, the school nurse, or the NHS for things like screening, vaccinations, health/eye/ dental checks, Education Health, and Care Plan (EHCP) provision etc. and UK Health Security Agency about certain contagious infections our pupils come into contact with.
- Government departments like UK Health Security Agency, local authority public health and District Council Environmental Health Departments to comply with the law and support public health action;
- Voluntary and charitable organisations (with your permission only), such as Barnardo's, our local Foodbank and similar organisations who can offer families practical help and support.
- third parties as listed in Appendix 6 of the Data Protection policy (KSMAT/STAT/023).

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Sharing with Youth Support Services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 5076B of the Education Act 1996.

This enables them to provide youth support services and careers advice.

The information shared is limited to the child's name, address and date of birth and the name and address of a parent/guardian. Consent to share this data is not required from a parent or guardian, but we do need parental consent to share any other information relevant to the provision of youth support services.

Data is securely transferred to the youth support service via either telephone or encrypted emails and is stored within school digitally (the data is stored in either our MIS System or on spreadsheets which are store in a secure area on the school network) and held by Inspira until the pupil reaches their 19th (or 24th if SEND) birthday.

Pupils aged 16+

We will also share certain information about pupils with our local authority and/or provider of youth support services as they have responsibilities in relation or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- Post 16 education and training providers;
- Youth support services;
- Careers advisers.

The information shared is limited to the pupil's name, address, and date of birth and the name and address of a parent or guardian. Consent to share this data is not required from a parent or guardian, but we do need a pupil's consent to share any other information about them that is relevant to the provision of youth support services. Data is securely transferred to the youth support service via either telephone or encrypted emails and is stored within school digitally (the data is stored in either our MIS System or on spreadsheets which are store in a secure area on the school network.) and held by Inspira until the pupil reaches their 19th (or 24th if SEND) birthday.

For more information about services for young people, please visit the local authority website.

Department for Education

We are required to share information about our pupils with the DfE directly or via our local authority for the purpose of statutory data collections, under the following legislation:

- section 29(3) and section 537A of the [Education Act 1996](#);
 - the [Education \(School Performance Information\)\(England\) Regulations 2007](#);
 - regulations 5 and 8 of the [School Information \(England\) Regulations 2008](#);
 - the [Education \(Pupil Registration\) \(England\) Regulations 2006](#);
 - [section 83 of the Children Act 1989](#) (for monitoring and research purposes); and
- for census purposes under regulation 5 of The [Education \(Information About Individual Pupils\) \(England\) Regulations 2013](#).

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current [government security policy framework](#).

For more information, please see the section on 'How Government uses your data' below.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Requesting access to your personal data

Under UK GDPR, parents, carers, and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact the school's Head Teacher.

Depending on which lawful basis above was used to process the data, you may also have the right to:

- ask us for access to information about you that we hold
- have your personal data rectified if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>. For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice below.

Contact

If you would like to discuss anything in this privacy notice, please contact Mrs Ruth Lawler, Data Protection Officer on 017687 72605.

Withdrawal of consent and the right to lodge a complaint

Where we are processing your personal data with your consent, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Mrs Ruth Lawler, Data Protection Officer on 017687 72605.

Last updated

This privacy notice was compiled using [DfE advice and model documents](#). We may need to review it periodically, so we recommend that you revisit this information from time to time.

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- Underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school;
- Informs 'short term' education policy monitoring and school accountability and intervention (for example school GCSE results or Pupil Progress measures);
- Supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school).

Data collection requirements

To find out more about the data collection requirements placed on us by the DfE (for example, via the school census) go to www.gov.uk/education/data-collection-and-censuses-for-schools.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the DfE and contains information about pupils in schools in England. It provides invaluable evidence on educational performances to inform independent research, as well as studies commissioned by the DfE.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-mpd-privacy-notice/national-pupil-database-mpd-privacy-notice>

Sharing by the DfE

The law allows the DfE to share pupils' personal data with certain third parties, including:

- Schools and local authorities;
- Researchers;
- Organisations connected with promoting the education of wellbeing of children in England;
- Other government departments and agencies;
- Organisations fighting or identifying crime.

For more information about the DfE data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>.

Organisations fighting or identifying crime may use their legal powers to contact the DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the DfE has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police, please visit the following website: <https://www.gov.uk/government/publications/dfe-external-data-shares>.

How to find out what personal information the DfE holds about you

Under the terms of the Data Protection Act 2018, you are entitled to ask the DfE:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they're holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, please make a 'subject access request' to them.

Find out how in the DfE's personal information charter published at:

www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the DfE go to: www.gov.uk/contact-dfe.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Privacy Notice: How we use School Workforce Information in Keswick School MAT

Keswick School Multi Academy Trust is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of workforce information that we process:

- Personal identifiers such as name, address, contact details, employee or teacher number, national insurance number and image;
- Financial information like bank account, pension, benefits, insurance, and similar detail;
- Biometric Data is collected to facilitate school access systems;
- Special categories of data like medical information for emergency or occupational health reasons; criminal conviction or social care action information for legal and safeguarding reasons; and protected characteristics information like gender, age, ethnic group etc.
- Special categories of data like medical information for emergency or occupational health reasons; criminal conviction or social care action information for legal and safeguarding reasons; and protected characteristics information like gender, age, ethnic group etc.
- Work absence information such as number of absences and reasons;
- Qualifications and, where relevant, subjects taught;
- CCTV recordings to protect the safety and security of children, staff and the school site.

Why we collect and use workforce information

We use school workforce data to:

- a) provide us with a comprehensive picture of our workforce, how it is deployed, how it can be developed, and kept safe;
- b) recruit appropriately and to inform the development of recruitment and retention policies;
- c) enable individuals to be evaluated and developed in their career and be paid
- d) meet statutory duties placed on us by HMRC, the Home Office, Department for Education, Department of Work and Pensions, UK Health Security Agency etc.
- e) enable individuals to access premises or services we control e.g. system logins, using biometric recognition;
- f) celebrate or promote school, for scientific interest, or to record our own school history.

Under UK GDPR, the lawful bases we rely on for processing personal workforce information are:

- to enter into or carry out a contract (mainly reasons b, c, and e above) e.g. to employ people or buy services for people to use.
- to comply with the law (mainly reasons b, c, and d above) e.g. recording sickness absence for benefits purposes, data sharing with child protection partners like social care, the NHS, and the Local Authority.
- to protect vital interests (mainly reason a above) e.g., allergy or other health information,
- having consent (mainly reasons e, and f above, and to process ethnicity data) e.g., use images and names in publicity (if another basis does not apply), or use biometric data as an identifier.

When we process special category data like medical information, biometrics, or criminal history, we need to have one lawful basis from the list above *and* one of the following list:

- having consent (mainly reasons a, d, and e above) e.g., to use biometric controlled catering services or referral to occupational health or other support services.
- to comply with the law (mainly reason d above) e.g., pre-employment criminal record checks, providing reasonable adjustments for work or interview.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- for preventative or occupational medicine or to assess the work capacity of an employee or to improve public health (mainly reason a above) e.g., report notifiable diseases to local or national government departments;
- to make or defend legal claims (mainly reason d above) e.g., some special educational needs records which include details about the staff involved, and all accident records etc.

Collecting workforce information

We collect personal information via numerous sources which are all retained securely. Information is only collected if it serves a purpose.

Most of the information we ask for is required by law or necessary so we can run the school effectively and some of it is voluntary. To comply with UK GDPR, if you have a choice about providing information, we will tell you when we ask for it. We will also tell you what to do if you do not want to share this information with us.

Storing workforce information

We hold data securely for the set amount of time indicated in our Records Management Policy (KSMAT/STAT/020). For more information on how we keep your data safe, please see the Data Protection policy (KSMAT/STAT/023).

Who we share this workforce information with

We do not share information about our workforce with anyone without consent unless the law and our policies allow us to do so. The laws listed in this notice that require us to collect information also require us to share it. Data is transferred securely by hand delivery or registered post, via a government data transfer system like School to School, via a contractor’s secure data sharing system like our online school trips safety system, and sometimes in other secure ways.

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring (see next section).

We routinely share this information with:

- Other parts of our MAT to monitor and share practice, benchmark locally, and to make decisions about workforce distribution and development.
- our payroll and pensions service provider to pay people;
- the Local Government Pension scheme (Your Pension Service) to manage pension contributions;
- HMRC for legal and tax reasons;
- organisations involved with our children like the local authority or other partner professionals who need the names, job titles, contact details and perhaps qualifications of our employees, the places we take children to on trips who might need more personal information like next of kin and medical needs, and workforce development organisations like training providers;
- Government departments like UK Health Security Agency, local authority public health, and District Council Environmental Health Departments to comply with the law and support public health action;
- Occupational Health and similar staff support services only with the consent of the individual.
- the Department for Education (DfE) – School workforce census only.
- other schools or organisations following reference requests
- other public services that have a lawful right to collect workforce information
- third parties listed in Appendix 6 of the DPA policy (KSMAT/STAT/023).

Department for Education (DfE) and our Local Authority

The Department for Education (DfE) collects personal data from education settings and local authorities via various statutory data collections.

The law requires us to share information about our school workforce with the Department for Education (DfE) for the purpose of those data collections, and with our local authority, under section 5 of the [Education \(Supply of Information about the School Workforce\) \(England\) Regulations 2007](#) and amendments.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under UK GDPR, you have the right to request access to information about you that we hold. To make a request for your personal information, please contact the school's Head Teacher.

Depending on which lawful basis above was used to process the data, you may also have a right to:

- ask us for access to information about you that we hold
- have your personal data rectified if it is inaccurate or incomplete
- request the deletion or removal of personal data where there is no compelling reason for its continued processing
- restrict our processing of your personal data (i.e., permitting its storage but no further processing)
- object to direct marketing (including profiling) and processing for the purposes of scientific/historical research and statistics
- be subject to decisions based purely on automated processing where it produces a legal or similarly significant effect on you.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

For further information on how to request access to personal information held centrally by DfE, please see the 'How Government uses your data' section of this notice.

Withdrawal of consent and the right to lodge a complaint

If we are only processing your personal data because you consented, you have the right to withdraw that consent. If you change your mind, or you are unhappy with our use of your personal data, please let us know by contacting Mrs Ruth Lawler, Data Protection Officer, 017687 72605.

Last updated

This privacy notice was compiled using [DfE advice and model documents](#). We may need to review it periodically, so we recommend that you revisit this information from time to time.

Contact

If you would like to discuss anything in this privacy notice, please contact: Mrs Ruth Lawler, Data Protection Officer, 017687 72605.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-census-for-schools>.

Sharing by the Department

The department may share information about school employees with third parties who promote the education or well-being of the effective deployment of school staff in England by:

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data.

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

How to find out what personal information DfE hold about you

Under the terms of the Data Protection Act 2018, you’re entitled to ask the Department:

- if they are processing your personal data
- for a description of the data they hold about you
- the reasons they’re holding it and any recipient it may be disclosed to
- for a copy of your personal data and any details of its source

If you want to see the personal data held about you by the DfE, you should make a ‘subject access request’. Further information on how to do this can be found in the DfE’s personal information charter published at: www.gov.uk/government/organisations/department-for-education/about/personal-information-charter

To contact the department: www.gov.uk/contact-dfe.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Privacy Notice: How we use visitors' information in Keswick School MAT

Keswick School Multi Academy Trust is the data controller under the UK General Data Protection Regulation (UK GDPR) for the use of personal data explained in this notice.

Personal data is any information that can be used to identify a living person, either on its own, or in combination with other pieces of data. Data processing includes the collection, use, and storage of data.

The categories of visitor information we process and why include:

- **Personal data** like your name, employer (if relevant to why you are here), and some location or other data e.g., the date & time you were here, your image on CCTV or an ID badge we give you, your contact number (if we will need to speak to you during or after your visit), your car registration if you are using our car park, and your device address (to allocate you an IP address) if you connect to our wi-fi.
- **Special categories** of data like a disability we need to accommodate or your DBS disclosure for safeguarding reasons.

We use this data to comply with the law (report an accident for example), deliver education and care, record our work with visitors when we need to (in meeting notes for example), for safety and security reasons, and to understand who visits us, why, and to improve the experience.

We will keep this information in a visitor management system for 6 years after your visit and it will not be shared with any other organisation. CCTV images are retained for one month. Depending on the purpose of your visit, information may be retained by us, including in the files of pupils or staff on paper and digitally. We have suitable physical and technical measures in place to protect it.

You have rights regarding your personal data as follows:

- you have the right to request access to your data
- you have the right to correct your data if it is incorrect.

If you want to know more or have concerns, or you want to exercise your rights, please contact Mrs Ruth Lawler, Data Protection Officer, 017687 72605.

Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Sample DPIA template



This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller's details:

Name of controller	
Subject/title of DPIA	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
	Remote, possible, or probable	Minimal, significant, or severe	Low, medium, or high

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	Low medium high	Yes/no

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

ACCESS TO PERSONAL DATA REQUEST

(Subject Access Request – SARS)

Enquirer's Surname		Enquirer's Forenames	
Enquirer's Address			
Enquirer's Postcode			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			YES / NO
If NO,			
Do you have the parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			YES / NO
If Yes,			
Name of child or children about whose personal data records you are enquiring			
Description of Concerns/Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name

Address

Postcode

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under the DPA (2018) and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of “Data Subject” (or Subject’s Parent) _____

Name of “Data Subject” (or Subject’s Parent) (PRINTED) _____

Dated _____

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Data Security User Checklist

This checklist applies to all Keswick School MAT staff, Governors and Directors and refers to personal data belonging to Keswick School MAT (as the data controller):

- Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.
- Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).
- Paper records containing personal data **must** be kept secure if they are taken off the school premises.
- MAT users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically (Online Safety Policy - KSMAT/STAT/034).
- Passwords **must** be alphanumeric, including one capital and one special character and be a minimum of 8 characters long to access the school network and Google Drive.
- MAT user names and passwords **must not** be shared.
- MAT electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.
- Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.
- Emails **must** be encrypted if they contain personal data and are being sent outside the EU (boarding pupils).
- Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
- Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- Visitors to MAT school premises containing special categories of personal data **must** be supervised at all times.
- Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
- Personal data **must not** be disclosed to any unauthorised third parties.

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

- Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
 - The device **must** be checked by an IT Technician before use;
 - It **must** be password protected;
 - It **must** be stored in a secure and safe place when not in use;
 - It **must not** be accessed by other users (e.g. family members) when out of a MAT school.
- Personal data **must** be securely deleted when no longer required.
- Personal electronic devices **must not** be used to hold personal data belonging to Keswick School MAT.
- Personal electronic devices **must** be password protected and have up-to-date, active anti-virus and anti-malware checking software before being used to access personal data belonging to Keswick School MAT via:
 - A password protected removable storage device;
 - The remote desktop protocol (i.e. remote access to the school network);
 - Google Drive (including Google docs, Google classroom etc.).
- Personal electronic devices that have been set to automatically log into the school network, school email accounts or Google drive that are lost or stolen **must** be reported to the DPO so that access to these systems can be reset.
- Google file stream can be used but copies of documents containing personal data **must not** be stored as local copies on the personal electronic device.
- If personal data is taken off Keswick School MAT premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.
- Before sharing personal data, Keswick School MAT staff/Governors/Directors **must** ensure:
 - They are allowed to share it;
 - That adequate security is in place to protect it;
 - Who will receive the personal data has been outlined in a privacy notice.
- Any personal data archived on disks **must** be kept securely in a lockable cabinet.
- Access to personal data in the School's Management Information System is limited by access rights. Access rights are reviewed on an annual basis or when job roles change.
- Pupils/staff personal paper files are stored in secure locked cupboards. Access is restricted to the Pastoral team, HR Officer and Headteacher.
- Keswick School MAT staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the DPA (2018).

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Third Party Suppliers with access to Keswick School MAT Personal Data

Company	Parents	Students	Staff	Other
Apple			✓	
Autodesk (Design Technology)		✓	✓	
Bandlab		✓	✓	
Blooket (MFL Department)		✓	✓	
CAPITA HR Solutions [Legacy Payroll Provider]			✓	
Circuit Wizard (Design Technology)		✓	✓	
Classcharts	✓	✓	✓	
Code.org		✓	✓	
Code Academy		✓	✓	
Compass+		✓	✓	
Corero [Legacy Finance Software]	✓	✓	✓	✓
CRB (Cashless Catering) [Including Biometric Data]		✓	✓	
CSI Literacy (Learning Support)		✓	✓	
Doddle		✓	✓	
Educake (Science)		✓	✓	
EduLink	✓	✓	✓	
Edukey (Learning Support)	✓	✓	✓	
Everlearner (PE Department)		✓	✓	
Exam Boards		✓	✓	
Flash Academy		✓	✓	
Focus software (Design Technology)		✓	✓	
GL Assessment (Testwise CAT Tests)		✓	✓	
Google		✓	✓	
Grammarly		✓	✓	
Groupcall	✓	✓	✓	
HCSS (Legacy Budgeting Software)			✓	
Hello Futures (Sixth Form)	✓	✓	✓	✓
IDL (Learning Support)		✓	✓	
Inspira (Careers)		✓		
IMP (Budgeting Software)			✓	
Impact (Catering)		✓	✓	
iPay Impact	✓	✓	✓	
Kahoot		✓	✓	
Language Gym (MFL Department)		✓	✓	
Language Nut (MFL Department)		✓	✓	
Locker		✓	✓	
Medical Authorities (Boarding)	✓	✓	✓	
Memrise (MFL Department)		✓	✓	
Microsoft Outlook (Emails)	✓	✓	✓	✓
MLS (Library Software)		✓	✓	

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

Notability		✓	✓	
NST Travel (school trips)	✓	✓	✓	✓
Parents Evening Booking System	✓	✓	✓	
PS Financials (Legacy Finance Software)	✓	✓	✓	✓
Quizlet (MFL Department)		✓	✓	
Reach (Boarding MIS Software)	✓	✓	✓	
Renaissance Learning (English Department)		✓	✓	
Satchel Pulse		✓	✓	
Scholar Pack (Primary MIS)	✓	✓	✓	
School ICT Services (SIMS Support)	✓	✓	✓	✓
Seneca (Revision resources)		✓	✓	
Techsoft (Design Technology)		✓	✓	
Timetable Rockstars (Maths)		✓	✓	
UCAS		✓	✓	
U-Explore (Start Careers Guidance Software)		✓	✓	
Unifrog (Sixth Form Department)		✓	✓	
Wonde (SIMS integration)	✓	✓	✓	✓
Work Experience Companies	✓	✓	✓	
Xero (Finance Software)	✓	✓	✓	✓
XYZ software (Design Technology)			✓	

Please note that where usernames are required for access Keswick School MAT use pupil's IT usernames rather than their actual names.

Third Party Suppliers - Letter to confirm compliance with DPA (2018)

Dear

As a third party supplier we need you to confirm that you have undertaken a review of your processes and procedures to comply with these new regulations. To continue with our commercial relationship we need confirmation of this and an agreement that the current contract will be amended to reflect this. Please complete the series of questions below and explain how you will comply.

28(3) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:

Requirement	Confirm consent and process
28(3)(a) process only on documented instructions, including regarding international transfers(unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);	
28(3)(b) ensure those processing personal data are under a confidentiality obligation (contractual or statutory);	

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	

28(3)(c) take all measures required under the security provisions which includes pseudonymising and encrypting personal data as appropriate;	
28(3)(d) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;	
28(3)(e) assist the controller in responding to requests from individuals (data subjects) exercising their rights;	
28(3)(f) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities;	
28(3)(g) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by UK law);	
28(3)(h) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.	

Ref:	Data Protection	Type:	Policy
Version:	05	Owner:	Executive Principal Keswick School Multi Academy Trust
Date:	March 2024	Status:	