DUDLEY ACADEMIES TRUST

GDPR/ Data Protection Policy

Issue number:	001
Approved by:	Board of Trustees
Date:	December 2018
Review date:	December 2019

Our mission: Working together we will develop inspirational schools which instil ambition and desire in young learners, open their minds, widen their horizons and equip them to succeed in a challenging world.

Contents

Introduction

Statement of Intent

It is the intention of Dudley Academies Trust to fulfil its obligations under the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018). It is the aim of the Trust to ensure that all staff are properly trained, fully informed of their obligations under the GDPR and are aware of their personal liabilities. Any employee deliberately acting outside of their recognised responsibilities may be subject to the Trust's disciplinary procedures.

Individuals whose information is held and processed by the Trust can be assured that their personal data with be treated with due care. This policy document applies only to information covered by the GDPR and relevant legislation impacting upon it. This policy will be a dynamic document that will be updated periodically according to the laws as set out by the European Union. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Definitions

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include an individual's: - Name (Including Initials) - Identification Number - Location Data - Online Identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection, including information about an individual's: - Racial or Ethnic Origin - Political Opinions - Religious or Philosophical Beliefs - Trade Union Membership - Genetics - Biometrics (such as fingertips, retina and iris patterns), where used for identification purposes

	- Health – physical or mental - Sex Life or Sexual Orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed
Data Controller	A person or an organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Fair Obtaining and Processing

The Trust will, as far as feasible, ensure that all individuals whose details are held are aware of the way in which that information will be held, used and disclosed. Individuals will be informed of the likely recipients of the information - whether the recipients are internal or external to the Trust. Processing within the Trust will be fair and lawful, individuals will not be misled as to the uses to which the Trust will put the information given. If a person feels they have been deceived or misled as to the reasons for which their information was collected, they should complain to the Data Protection Officer (DPO). Information regarding personal data, how and why it is collected, can be found within each school's respective Privacy Notice.

Information Uses and Processes

The Trust will not use or process personal information in any way that contravenes its notified purposes or in any way that would constitute a breach of the General Data Protection Regulation. Any new purposes introduced will, where appropriate, be notified to the individual and, if required by the law, their consent will be sought.

All staff using personal information within the Academy are told the limits of their authority to use and disclose such information. The Trust has a reporting structure to ensure that data protection policies and procedures are properly communicated throughout the Trust; all new purposes are documented and notified to the Information Commissioner.

Information Quality and Integrity

The Trust will not collect information from individuals where that information is excessive or irrelevant in relation to the notified purpose(s). Details collected will be adequate for the purpose and no more. Personal data, which becomes irrelevant or excessive, will be deleted. Information will only be held for as long as is necessary for the notified purpose(s). Where details of individuals are stored for long-term archive or historical reasons and where it is necessary to retain the personal detail within the records it will be done within the requirements of the legislation.

The Trust will ensure, as far as is feasible, that the information held is accurate and up to date. It is the intention of the Academy to check wherever possible the details given. Information received from third parties (i.e. neither the individual concerned nor the Academy) should carry a marker indicating the source. Where a person informs the Academy of a change of their own circumstances, such as home address or non-contentious data, their record(s) will be updated as soon as possible. Where the individual requests that information be changed and it is not possible to update it immediately, or where the new information needs to be checked for its accuracy or validity, it is recommended that a marker be placed on the disputed record indicating the nature of the problem.

Technical and Organisational Security

The Trust implements appropriate security measures as required under the GDPR. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place with visitors being received and supervised at all times within the Academy's buildings where information about individuals are stored.

Computer systems are installed with user-type profile type password controls and, where necessary, audit and access trails to establish that each user is fully authorised. In addition, employees are fully informed about overall security procedures and the importance of their role within those procedures. Manual filing systems should be held in secure locations and only accessed on a need-to-know basis. Electronic records should be held securely and safely in line with the Trust's Information Security Policy.

Details should only be disclosed on a needs basis within the Trust. Where details need to be passed outside the Trust, it is only done with the person's consent except where this is not possible or where required by law, allowed under the GDPR exemptions or where it is in the person's vital interests.

Subject Access/Subject Information Requests

Any person whose details are held / processed by the Trust has a general right to receive a copy of their own information. There are a few exceptions to this rule, such as information held for child protection or crime detection/prevention purposes, but most individuals will be able to have a copy of the information held on them. Any codes used in the record will be fully explained and any inaccurate, out of date, irrelevant or excessive information will be dealt with accordingly. Any Person/s who wish to access their data are to direct queries to the Data Protection Officer (DPO).

Legal Framework

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

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act (2000)
- The Education (Learner Information) (England) Regulations 2005 (As amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The policy will also have regard to the following guidance:
- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

Roles and Responsibilities

Governing Bodies

The governing board has overall responsibility for ensuring that our schools complies with all relevant data protection obligations. A GDPR lead will be appointed from the board of Trustees to liaise with the DPO on all matters relating to data protection. The board will also be updated, as a standing agenda item at each meeting, on any data breaches or major changes in policy.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy and developing related policies and guidelines where applicable. The DPO will inform and advise the Trust and its employees about their obligations to comply with the GDPR and other Data Protection laws. They will also monitor the Trust's compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits and providing the required training to staff members.

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

Sufficient resources will be provided to the DPO to ensure that they are able to meet their GDPR obligations. The DPO will report to the highest level of management at the Trust, which is the Chief Executive Officer (CEO). Each individual Academy will have a Data Protection Representative who will lead on Data Protection issues locally and will be advised and work together with the DPO

The DPO is the first point of contact for individuals whose data the school processes, and for the ICO:

Dudley Academies Trust – Data Protection Officer (DPO):
Mrs Rebecca Meacham
Dudley Academies Trust
Priory Villa, 3a Ednam Road
Dudley,

DY1 1HL

The contact details of the individual Academy Data Protection Representatives can be found on the Trust Privacy Notice.

Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) of the Trust acts as the representative of the data controller on a day-to-day basis.

School based Data Protection Representative (DPR)

The DPR will be based at each school and is responsible for:

- Supporting the DPO in the implementation of the policy and procedures on the ground.
- Monitoring processing activities within the school and highlighting areas of risk.
- Communicating with the DPO on areas of concern.
- Encouraging the change of behaviour towards a more aware environment on data security.

All Staff Members Employed by Dudley Academies Trust

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as change of address
- Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

The Principles of the General Data Protection Regulation

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

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard for the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific of historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles". As the Data Controller, it is the responsibility of Dudley Academies Trust to ensure that all of the above Principles are adhered to.

Collecting Personal Data

Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can comply with a legal obligation The data needs to be processed to ensure that vital interests of the individual, e.g. to protect a life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a Learner) has freely given clear consent

Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. These reasons will be disclosed to the individual upon data collection and can also be found in the respective school's Privacy Notice. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Retention Schedule (see Appendix 2).

Consent

Some data that we collect is subject to active consent by the data subject. Where consent is required, it must be a positive indication. Where consent is given, a record will be kept documenting how and when consent was given. Consent for the use of this data can be withdrawn by the individual at any time.

Sharing Personal Data

Personnel within the Trust will not normally share personal data with anyone else, but may do so where:

- There is an issue with a Learner or parent/carer that puts the safety of our staff at risk
- It is necessary to liaise with other agencies – where necessary we will seek consent
- Our suppliers or contractors need data to enable us to provide services to our staff and Learners – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law; in respect of all current suppliers or contractors, contact has been made by Dudley Academies Trust to ensure compliance with GDPR
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for, but not exhaustive of:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our Learners or staff. Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law. For an up to date list of who we share data with, see each respective school's Privacy Notice.

Subject Access Requests and other Rights of Individuals

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

1. Confirmation that their personal data is being processed
2. Access to a copy of the data
3. The purposes of the data processing
4. The categories of personal data concerned
5. Who the data has been, or will be, shared with
6. How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
7. The source of the data, if not the individual

Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual
Subject access requests must be submitted in writing; either by letter or email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of Learners at our school may not be granted without the express permission of the Learner. This is not a rule and a Learner's ability to understand their rights will always be judged on a case-by-case basis.

Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge

We will not disclose information if it:

- Might cause harm to the physical or mental health of the Learner or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will disclose to the individual the reasoning, and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the Individual

In accordance with the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Challenge processing which has been justified on the basis of public interest
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)
- Withdraw permission to processing of data that has been subject to consent at any time

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Parental Requests to see the Educational Record

Responsibility of the Trust

The Trust is responsible for a learner's educational record being made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this must be provided to them, also within 15 school days of that request being received. The governing body can charge a fee for the copy, but if they do this it must not be more than the cost of supply. The educational record will include the curricular record but also other information about the learner that may be kept by the school, such as details of behaviour and family background, the definition is given below.

The Educational Record

A learner's educational record is comprised of any record of information, other than information which is processed by a teacher solely for the teacher's own use, which:

- Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local authority (LA) and any special school not so maintained;
- Relates to any person who is or has been a learner at any such school; and originates from or was supplied by or on behalf of;
- Any employee of the Dudley Academies Trust which maintains the Academy (or former school) attended by the learner to whom the record relates;
- Where the school is a voluntary aided, foundation or foundation special school or a special school not maintained by an LA, any teacher or other employee at the school or at the learner's former school (including any educational psychologist engaged by the governing body under a contract for services),
- The learner to whom the record relates or a parent of that learner.
- Additionally it includes:

    - Any statement of special educational needs held in respect of the learner;
    - Any Personal Education Plan (PEP) held in respect of the learner. The PEP is the document initiated by children's social services when a child is taken into care and maintained by the child's school, which provides a record of educational needs, objectives and progress and achievements.
    - Information covered by the definition above falls within a variety of categories, including child protection records, records where a child has a statement of SEN and records regarding exclusions.

Biometric Recognition Systems

Learners

Where we use Learner's biometric data as part of an automated biometric recognition system, for example in the case of paying for school lunch, we will comply with the Protection of Freedoms Act 2012.

Parents/carers will be notified before any additional biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and Learners have the right to choose not to use the school's biometric system. Alternative means of accessing the relevant system will be provided for those Learners. For example, Learners can pay for school dinners using a dinner card.

Parents/carers and Learners can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time; we will ensure that any relevant data already captured is deleted

As required by law, if a Learner refuses to participate in, or continue to participate in, the processing of their biometric data; we will not process that data irrespective of any consent given by the Learner's parent(s)/carer(s).

Staff Members

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

CCTV and Headcams

Across all of our schools, both CCTV and in some cases Head-Cameras are used in various locations to ensure the safety and security of our respective sites. In both these instances, we will adhere to the Information Commissioner's Office (ICO) code of practice for the use of these cameras.

(https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf)

We do not need to ask individual's permission to use these cameras, but we make it clear where individuals are being recorded. Security cameras, both stationary and on security personnel, are clearly visible and where necessary accompanied by prominent signs explaining that the cameras are in use.

Any enquiries about the CCTV system or use of head-cameras should be directed to the DPO. A separate policy on the use of CCTV and Headcams can be found on the Trust website.

Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, for photographs and videos to be taken of Learners for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and Learner. Where we don't need parental consent, we will clearly explain to the Learner how the photograph and/or video will be used.

Uses of photographs and videos include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc. (consent not required)
- Outside of school by external agencies such as the school photographer, newspapers, campaigns (through consent)
- Online on our school website or social media pages (through consent)

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further. When using photographs and videos in this way, we will not accompany them with any other personal information about the child, to ensure they cannot be identified. See our photograph policy for more information on our use of photographs and videos.

Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to our privacy measures and make sure we are compliant
- Maintaining records of our processing activities including:
- For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
- For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where highly confidential personal information needs to be taken off site, appropriate measures to ensure its safety will be taken
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and Learners are reminded to change their passwords at regular intervals
- Encryption software is used to protect portable devices
- Staff, Learners or governors will not store personal information on their personal devices and rather use the school's Office 365 environment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of Learners eligible for the Learner premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about Learners

Training

- All staff and governors are provided with data protection training as part of their induction process.
- Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed every **1/2 years** and shared with the full governing board.

Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy Notices for each respective School
- Photograph and Video Policy
- CCTV and Headcam Policy
- Safeguarding Policy
- Acceptable Use of ICT Policy

Appendix 1: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
- Lost
- Stolen
- Destroyed
- Altered
- Disclosed or
- made available where it should not have been o Made available to unauthorised people
- The DPO will alert the CEO of the Trust and the Data Protection Representative on the CAT Board of Trustees.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

- (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
- Loss of control over their data o Discrimination o Identify theft or fraud o Financial loss
- Unauthorised reversal of pseudonymisation (for example, key-coding) o Damage to reputation o Loss of confidentiality
- Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on our GDPRis software system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out: o A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
    - If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
    - The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the: o Facts and cause o Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- Records of all breaches will be stored on our GDPRis software system
- The DPO and CEO will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Appendix 2: Data Retention Schedule

Governors

Governors					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Minutes					
Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting	Transfer to Archives

Inspection copies	No		Date of meeting + 3 years	DESTROY [If these minutes contain any sensitive personal information they should be shredded]	
Agendas	No		Date of meeting	DESTROY	
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Annual Parents' meeting papers	No		Date of meeting + 6 years	Retain in school for 6 years from date of meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Instruments of Government	No		Permanent	Retain in school whilst school is open	Transfer to Archives when the school has closed
Trusts and Endowments	No		Permanent	Retain in school whilst operationally required	Transfer to Archives

Action Plans	No		Date of action plan + 3 years	DESTROY	It may be appropriate to offer to the Archives for a sample to be taken if the school has been through a difficult period
Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (this includes if the expired policy is part of a past decision making process)	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years Review for further retention in the case of contentious disputes Destroy routine complaints	
Annual Reports required by the Department for Education and Skills	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

Proposals for schools to become, or be established as Specialist Status schools	No		Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

Management

Management					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Log Books	Yes[1]		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives

[1] From January 1st 2005 subject access is permitted into unstructured filing systems and log books and other records created within the school containing details about the activities of individual Learners and members of staff will become subject to the Data Protection Act 1998.

Minutes of the Senior Management Team and other internal administrative bodies	Yes[1]		Date of meeting + 5 years	Retain in the school for 5 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Reports made by the head teacher or the management team	Yes[1]		Date of report + 3 years	Retain in the school for 3 years from meeting	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	Yes[1]		Closure of file + 6 years	DESTROY If these records contain sensitive information they should be shredded	
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	DESTROY If these records contain sensitive information they should be shredded	

Professional development plans	Yes		Closure + 6 years	SHRED	
School development plans	No		Closure + 6 years	Review	Offer to the Archives

Learners

Learners					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry.	Transfer to the Archives
Attendance registers	Yes		Date of register + 3 years	DESTROY [If these records are retained electronically any back up copies should be destroyed at the same time]	

Learner record cards	Yes				
Primary			Retain for the time which the Learner remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service	
Secondary			DOB of the Learner + 25 years[2]	SHRED	
Learner files	Yes				
Primary			Retain for the time which the Learner remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school. In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service	

[2] In the case of exclusion it may be appropriate to transfer the record to the Behaviour Service

Secondary			DOB of the Learner + 25 years[3]	SHRED	
Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the Learner + 25 year[4]	SHRED	
Letters authorising absence	No		Date of absence + 2 years	SHRED	
Absence books			Current year + 6 years	SHRED	
Examination results	Yes				
Public	No		Year of examinations + 6 years	DESTROY	Any certificates left unclaimed should be returned to the appropriate Examination Board

[3] As above
[4] As above

Internal examination results	Yes		Current year + 5 years[5]	DESTROY	
Any other records created in the course of contact with Learners	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or DESTROY	
Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	
Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	DESTROY unless legal action is pending	
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	DESTROY unless legal action is pending	

[5] If these records are retained on the Learner file or in their National Record of Achievement they need only be kept for as long as operationally necessary.

Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	DESTROY unless legal action is pending	
Children SEN Files	Yes		Closure + 35 years	DESTROY unless legal action is pending	

Curriculum

Curriculum					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
Curriculum development	No		Current year + 6 years	DESTROY	
Curriculum returns	No		Current year + 3 years	DESTROY	

School syllabus	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	
Learners' work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or DESTROY	

Examination results	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
SATS records	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
PANDA reports	Yes		Current year + 6 years	DESTROY [These records should be shredded]	
Value added records	Yes		Current year + 6 years	DESTROY [These records should be shredded]	

Personnel

Personnel					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SHRED	

Staff Personal files	Yes[6]		Termination + 7 years	SHRED	
Interview notes and recruitment records	Yes		Date of interview + 6 months	SHRED	
Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SHRED [by the designates member of staff]	
Disciplinary proceedings:	Yes		Please note that all these retention periods where the warning relates to child protection issues may change in light of any recommendations made by the Bichard Inquiry.		
Oral warning			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.	
written warning – level one			Date of warning + 6 months	SHRED If this is placed on a personal file, it must be weeded from the file.	

[6] These files should be subject to KCC's open file policy where the employees are employed by RECORDS MANAGEMENT SOCIETY OF GREAT BRITAIN as the Local Education Authority.

written warning – level two			Date of warning + 12 months	SHRED If this is placed on a personal file, it must be weeded from the file.	
final warning			Date of warning + 18 months	SHRED If this is placed on a personal file, it must be weeded from the file.	
case not found			DESTROY immediately at the conclusion of the case		
Records relating to accident/injury at work	Yes		Date of incident + 12 years	Review at the end of this period. In the case of serious accidents a further retention period will need to be applied	
Annual appraisal/assessment records	No		Current year + 5 years	SHRED	
Salary cards	Yes		Last date of employment + 85 years	SHRED	

Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year, +3yrs	SHRED	
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SHRED	

Health and Safety

Health and Safety					
Basic file description	**Data Protection Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**	
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	DESTROY	

Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980			
Adults	Yes		Current year + 3 years	SHRED	
Children	Yes		DOB + 25 years[7]	SHRED	
COSHH			Current year + 10 years	Review [where appropriate an additional retention period may be allocated]	
Incident reports	Yes		Current year + 20 years	SHRED	

[7] A child may make a claim for negligence for 7 years from their 18th birthday. To ensure that all records are kept until the Learner reaches the age of 25 this retention period has been applied.

Policy Statements			Date of expiry + 1 year	DESTROY	
Risk Assessments			Current year + 3 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with asbestos			Last action + 40 years	DESTROY	
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	DESTROY	
Fire Precautions log books			Current year + 6 years	DESTROY	

Administrative

Administrative					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Employer's Liability certificate			Permanent whilst the school is open	DESTROY once the school has closed	
Inventories of equipment and furniture			Current year + 6 years	DESTROY	
General file series			Current year + 5 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

School brochure/prospectus			Current year + 3 years		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Circulars (staff/parents/Learners)			Current year + 1 year	DESTROY	
Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Visitors' book			Current year + 2 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
PTA/Old Learners' Associations			Current year + 6 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

Finance

Finance					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Annual Accounts		Financial Regulations	Current year + 6 years		Offer to the Archives
Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Contracts					
under seal			Contract completion date + 12 years	SHRED	

under signature			Contract completion date + 6 years	SHRED	
monitoring records			Current year + 2 years	SHRED	
Copy orders			Current year + 2 years	SHRED	
Budget reports, budget monitoring etc			Current year + 3 years	SHRED	
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SHRED	
Annual Budget and background papers			Current year + 6 years	SHRED	
Order books and requisitions			Current year + 6 years	SHRED	
Delivery Documentation			Current year + 6 years	SHRED	

Debtors' Records		Limitation Act 1980	Current year + 6 years	SHRED	
School Fund – Cheque books			Current year + 3 years	SHRED	
School Fund – Paying in books			Current year + 6 years	SHRED	
School Fund – Ledger			Current year + 6 years	SHRED	
School Fund – Invoices			Current year + 6 years	SHRED	
School Fund – Receipts			Current year + 6 years	SHRED	
School Fund – Bank statements			Current year + 6 years	SHRED	
School Fund – School Journey books			Current year + 6 years	SHRED	
Applications for free school meals, travel, uniforms etc			Whilst child at school	SHRED	

Learner grant applications			Current year + 3 years	SHRED	
Free school meals registers	Yes	Financial Regulations	Current year + 6 years	SHRED	
Petty cash books		Financial Regulations	Current year + 6 years	SHRED	

Property

Property					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Title Deeds			Permanent	These should follow the property	Offer to Archives
Plans			Permanent	Retain in school whilst operational then	Offer to Archives
Maintenance and contractors		Financial Regulations	Current year + 6 years	DESTROY	

Leases			Expiry of lease + 6 years	DESTROY	
Lettings			Current year + 3 years	DESTROY	
Burglary, theft and vandalism report forms			Current year + 6 years	SHRED	
Maintenance log books			Last entry + 10 years	DESTROY	
Contractors' Reports			Current year + 6 years	DESTROY	

LEA

LEA					
Basic file description	Data Protection Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SHRED	

Attendance returns	Yes		Current year + 1 year	DESTROY	
Circulars from LEA			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

DfES

DfES					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
HMI reports			These do not need to be kept any longer		Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

Returns			Current year + 6 years	DESTROY	
Circulars from DfES			Whilst operationally required	Review to see whether a further retention period is required	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]

Connexions

Connexions					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Service level agreements			Until superseded	SHRED	
Work Experience agreement			DOB of child + 18 years	SHRED	

School Meals

School Meals					
Basic file description	Data Prot Issues	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record	
Dinner Register			Current year + 3 years	SHRED	
School Meals Summary Sheets			Current year + 3 years	SHRED	