PORTICO
ACADEMY TRUST

opening doors, unlocking potential

Data Protection Policy

(to be read in conjunction with Records Management Policy)

Date Created:	September 2020
Next Review Date:	September 2024

Signature of Chair of Trustees _____ Date _____	Signature of Chief Executive Officer _____ Date _____

Introduction:

Portico Academy Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.
This policy applies to all personal data, regardless of whether it is in paper or electronic format.

Legislation and Guidance:
This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.
It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.
In addition, this policy complies with our funding agreement and articles of association.

Definitions:

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the 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 memberships • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical and 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 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

[1] (For further information about the collection and use of data refer to our Portico Privacy Agreements. These documents can be found on each of our academy's websites:

Roles and Responsibilities:
This policy applies to all staff employed by Portico Academy Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

Board of Trustees
The Portico Academy Trust Board of Trustees has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

Data protection officer
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.
They will provide an annual report of their activities directly to the Portico Academy Trust Board of Trustees and, where relevant, report to the board their advice and recommendations on academy data protection issues.
The DPO is also the first point of contact for individuals whose data the academy processes, and for the ICO.
Full details of the DPO's responsibilities are set out in their job description.

Our DPO is **Joanne Jarvis** and is contactable via **01702 987890**

Along with our DPO we have dedicated Data Champions for each academy within the Trust.

Head
The head acts as the representative of the data controller on a day-to-day basis.

All staff
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 a 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.

GDPR Principles:

The GDPR is based on data protection principles that our academies must comply with.
The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

Collecting Personal Data:

Lawfulness, fairness and transparency

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

- The data needs to be processed so that the academy 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 the vital interests of the individual e.g to protect someone's 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 individuals rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018

Academies

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except in certain Safeguarding or Child Protection circumstances. See Portico Safeguarding Policy for more information)

Limitation, minimisation and accuracy

We will only collect personal data for a specified, explicit and legitimate reason. We will explain these reasons to the individuals when we first collect their data.
If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individual 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 timescales set out on www.IRMS.org.uk/page/schoolstoolkit

Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – 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
    - 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:

- 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 respond to an emergency situation that affects any of our pupils 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.

Subject Access Requests and Other Rights to 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:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- 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, email or fax to the DPO. They should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

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 below the age of 12 are generally not 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 pupils at Portico Academy Trust may be granted without the express permission of the pupil. This is not a rule and a pupil'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 individuals 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
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil 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 tell the individual why and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- 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
- Challenge processing which has been justified on the basis of public interest
- 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 the transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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.

CCTV:

We use CCTV in various locations on each academy site to ensure staff/pupils and visitors remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask the individuals permission to use CCTV but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Photographs and Videos:

As part of the Portico Academy Trust activities, we may take photographs and record images of individuals within the Trust.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in academy magazines, brochures, newsletters etc
- Outside of the academy by external agencies such as the external school photographers, newspapers, campaigns
- Online on the Portico Academy Trust website or social media pages.

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.

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 (see section 6)
- Completing privacy impact assessments where the schools 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
- Annual updates for members of staff on changes to 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 test 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 Portico Academy Trust 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, and 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 personal information needs to be taken off site, staff must sign it in and out from the school office
- 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 pupils are reminded to change their passwords at regular intervals.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and taken reasonable steps to ensure it is stored securely and adequately protected.
- All staff, pupils or governors who use pen drives should ensure they are school issued encrypted devices to ensure secure storage of any personal data.

Personal data breaches:
Our academies will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected 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 pupils eligible for the pupil premium
- Identifiable safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils.

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 schools 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 the Portico Academy Trust practice. Otherwise, or from then on, this policy will be reviewed every year and shared with the Board of Trustees.

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
    - Made available to unauthorised people
- The DPO will alert the Head, CEO and the Chair of the Trust
- 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 again
- 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, mental, material or non-material damage (e.g. emotional distress) including through:
    - Loss of control over their data
    - Discrimination
    - Identity theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - 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 the academies' computer file 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:
    - 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 side 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:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for an individual)

  Records of all breaches will be stored on the academies computer file system.
- The DPO, Head 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.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data(sensitive information)is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who received personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask ICT support to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will ensure the Trust receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.

- Paper records should be shredded using a cross-cutting shredder
- CDs / DVDs / Floppy Disks should be cut into pieces
- Audio / Video Tapes and Fax Rolls should be dismantled and shredded
- Hard Disks should be dismantled and sanded, or disposed through a secure disposal company.
- Emails should be reviewed regularly and deleted folders emptied on a regular basis.

An internal log should be kept by the Data Protection Officer with input from the Data Champions at each academy to keep a record of when large scale destructions of data are made, both for an audit trail and also to ensure that the retention policy is being upheld.

Appendix 3: Clear Desk Policy

To improve the security and confidentiality of information, Portico Academy Trust has adopted a Clear Desk Policy for computer and printer workstations.

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

A Clear Desk Policy is an important security and privacy control and necessary for ISO 27001/17799 compliance.

Scope
This policy applies to all permanent, temporary, and contracted staff working at Portico Academy Trust.

Best Practice
Whenever a desk is unoccupied for an extended period of time the following is recommended:

- All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives.
- All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins. Under no circumstances should this information be placed in regular waste paper bins.
- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
- Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
- Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
- Printers and fax machines should be treated with the same care under this policy:
- Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, the “Locked Print” functionality should be used.
- All paperwork left over at the end of the work day will be properly disposed of.

Appendix 4: Retention schedule for Personal Data

Basic file description	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
Governing Body/Board of Trustees			
Records relating to complaints dealt with by the Governing Body/Board of Trustees		Date of the resolution of the complaint + a minimum of 6 years then review for the further retention in case of contentious disputes	SECURE disposal
Headteacher and Senior Management Team			
Professional Development Plans		Life of the plan + 6 years	SECURE disposal
Admissions Process			
Admissions – if the admission is successful	School Admissions Code.	Date of admission + 1 year	SECURE disposal
Admissions – if the appeal is unsuccessful	School Admissions Code.	Resolution of case + 1 year	SECURE disposal
Register of Admissions	School Attendance:	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made	REVIEW. Schools may wish to consider keeping admission register permanently as often schools receive enquiries from past pupils confirm the dates they attended the school
Proofs of address supplied by Parents as part of admissions process	School Admissions Code.	Current year + 1 year	SECURE disposal
Operational administration			
Visitors books and signing in sheets		Current year + 6 years then REVIEW	SECURE disposal
Recruitment			
All records leading up to the appointment of a new headteacher		Date of appointment + 6 years	SECURE disposal
All records leading up to the appointment of a new member of staff – unsuccessful candidates		Date of appointment of successful candidate + 6 months	SECURE disposal
All records leading up to appointment of a new member of staff – successful candidate		All relevant information should be added to the staff personal file and all other information retained for 6 months	SECURE disposal

Proofs of identity collected as part of the process of checking 'portable' enhanced DBS disclosure		Where possible these should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the member of staffs personal file	SECURE disposal
Pre-employment vetting information – evidence proving the right to work in the UK	An employer's guide to right to work checks	Where possible these documents should be added to the staff personal file, but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	SECURE disposal
Operational Staff Management			
Staff Personal file	Limitation Act 1980	Termination of employment + 6 years	SECURE disposal
Timesheets		Current year + 6 years	SECURE disposal
Annual appraisal/assessment records		Current year + 5 years	SECURE disposal
Management of Disciplinary and Grievance Processes			
Allegation of a child protection nature against a member of staff including where the allegation is unfounded	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note: allegations that are found to be malicious should be removed from personnel files. If found; they are to be kept on the file and a copy provided to the person concerned	SECURE disposal
Disciplinary Proceedings		Date of warning + 18 months	SECURE disposal
Records relating to accident/injury at work		Date of incident + 12 years	SECURE disposal

Accident reporting	Social Security (Claims and Payments) Regulations Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of incident + 6 years for adults, + 25 from DOB from child	SECURE disposal
Maternity pay records	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE disposal
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995		Current year + 6 years	SECURE disposal
Accounts and Statement including Budget Management			
Student Grant applications		Current year + 3 years	SECURE disposal
School Meals Management			
Free School Meals Registers		Current year + 6 years	SECURE disposal
School Meals Registers		Current year + 3 years	SECURE disposal
Pupil's Educational Record			
Pupil's Educational Record required by The Education (Pupil Information) Regulations 2005	The Education (Pupil Information) (England) Regulations 2005	Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period.

			/cont …. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
Examination Results – Internal		This information should be added to the pupil file	SECURE disposal
Child Protection information held on pupil file	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	If any records relating to child protection issues are placed on the pupil file, they should be in a sealed envelope and then retained for the same period of time as the pupil file	SECURE disposal – these records MUST be shredded
Child protection information held in separate files	"Keeping children safe in education Statutory guidance for schools and colleges"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	DOB of the child + 25 years	SECURE disposal – these records MUST be shredded
Attendance			
Attendance registers	School Attendance:	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE disposal

Correspondence relating to authorised absence	Education Act 1996 Section 7	Current academic year + 2 years	SECURE disposal

Special Educational Needs			
Special Educational Needs files, reviews and individual education plans	Limitation Act 1980	DOB + 25 years	SECURE disposal
Statement maintained under section 234 of the Education Ace 1990 and any amendments made to the statement	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DOB + 25 years	SECURE disposal
Advice and information provided to parents regarding educational needs	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DOB + 25 years	SECURE disposal
Accessibility Strategy	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	DOB + 25 years	SECURE disposal
Published Admission number (PAN) reports		Current year + 6 years	SECURE disposal
Value added and contextual data		Current year + 6 years	SECURE disposal
Self-evaluation forms		Current year + 6 years	SECURE disposal
Educational Visits outside the classroom			
Parental consent forms for school trips where there has been no incident		Conclusion of the Trip	SECURE disposal
Parental consent forms for school trips where there has been a major incident	Limitation Act 1980	DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE disposal