Data Protection Policy (including Privacy Notices)

Approved by the Governing Body in:

Autumn 2018

Aims

Monkfield Park aims to ensure that all personal data collected about staff, children, 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. 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) • Unique pupil number • Address • Parents' national insurance number • Contact details and preference (contact telephone numbers, email addresses, addresses) • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, mental, economic, cultural or social identity. N.B. This list is not exhaustive and reference should be made to Monkfield Park Privacy notices for workforce information and pupil information (see appendices 2 & 3).
Sensitive personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Religious or philosophical beliefs

	• Language • Nationality • Country of birth • Free school meal eligibility • Trade union membership N.B. This list is not exhaustive and reference should be made to Monkfield Park Privacy notices for workforce information and pupil information (see appendices 2 & 3).
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.

The data controller

Monkfield Park processes personal data relating to parents, children, staff, governors, visitors and others, and therefore is a data controller.

Monkfield Park is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

Data protection principles

The GDPR is based on data protection principles that Monkfield Park 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 Monkfield Park aims to comply with these principles.

Roles and responsibilities

This policy applies to **all staff** employed by Monkfield Park, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

The governing body has overall responsibility for ensuring that Monkfield Park complies with all relevant data protection obligations.

The Headteacher is responsible for overseeing the implementation of this policy, monitoring Monkfield Park's 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 governing body and, where relevant, report to them their advice and recommendations on Monkfield Park's data protection issues.

The Headteacher is also the first point of contact for individuals whose data Monkfield Park processes, and for the ICO. The Headteacher will liaise with the Data Protection Officer (see contact details below), where necessary.

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

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing Monkfield Park of any changes to their personal data, such as a change of address
- Contacting the Headteacher 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

Collecting personal data

Lawfulness, fairness and transparency

Monkfield Park will only process personal data where it has one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that Monkfield Park can **fulfil a contract** with the individual, or the individual has asked Monkfield Park to take specific steps before entering into a contract
- The data needs to be processed so that Monkfield Park 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 Monkfield Park 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 Monkfield Park 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 child) has freely given clear **consent**

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

If Monkfield Park offers online services to children, such as classroom apps, it intends to rely on consent as a basis for processing, Monkfield Park will get parental consent (except for online counselling and preventive services).

Limitation, minimisation and accuracy

Monkfield Park will only collect personal data for specified, explicit and legitimate reasons. Monkfield Park will explain these reasons to the individuals when data is first collected.

If Monkfield Park wants to use personal data for reasons other than those given when it first obtains it, it will inform the individuals concerned before they 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 Monkfield Park's record retention schedule (see appendix 4).

Sharing personal data

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

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- Monkfield Park needs to liaise with other agencies – consent will be sought as necessary before doing this
- Monkfield Park suppliers or contractors need data to enable Monkfield Park to provide services to staff and children – for example, IT companies. When doing this, Monkfield Park 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 that Monkfield Park shares
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with Monkfield Park

Monkfield Park will also share personal data with law enforcement and government bodies where it is 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
- Legal proceedings
- Where 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

Monkfield Park may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any children or staff.

Where Monkfield Park transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

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 Monkfield Park 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 Headteacher (who will liaise with 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 Headteacher.

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 Monkfield Park may be granted without the express permission of the child. This is not a rule and a child'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, Monkfield Park:

- 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

- May tell the individual that Monkfield Park will comply within 3 months of receipt of the request, where a request is complex or numerous. It will inform the individual of this within 1 month, and explain why the extension is necessary

Monkfield Park will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child 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, Monkfield Park 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 Monkfield Park refuses a request, it 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 Monkfield Park is collecting their data about how they use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask Monkfield Park 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 be 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 Headteacher, who will liaise with the DPO. If staff receive such a request, they must immediately forward it to the Headteacher.

Parental requests to see the educational record

Parents, or those with parental responsibility, do not have a legal right to access to their child's educational record (which includes most information about a child). If you wish to have access please put your request and reasons in writing to the Headteacher.

CCTV

Monkfield Park uses CCTV in various locations around the Monkfield Park site to ensure it remains safe. It will adhere to the ICO's code of practice for the use of CCTV.

Monkfield Park does not need to ask individual's permission to use CCTV, but it does make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

Photographs and videos

As part of Monkfield Park activities, photographs and recorded images of individuals may be taken within the setting.

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

Uses may include:

- Within Monkfield Park on notice boards and in Monkfield Park magazines, brochures, newsletters, etc.
- Outside of Monkfield Park by external agencies such as the school photographer, newspapers, campaigns
- Online on the Monkfield Park website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, Monkfield Park will delete the photograph or video and not distribute it further.

When using photographs and videos in this way, Monkfield Park will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Data protection by design and default

Monkfield Park will put measures in place to show that it has integrated data protection into all of its 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 Monkfield Park'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; Monkfield Park will also keep a record of attendance
- Regularly conducting reviews and audits to test Monkfield Park's privacy measures and ensure compliance
- Maintaining records of Monkfield Park's processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of Monkfield Park's DPO and all information Monkfield Park is required to share about how it uses and processes their personal data (via privacy notices)
    - For all personal data held by Monkfield Park, maintaining an internal record of the type of data, data subject, how and why data is used, any third-party recipients, how and why data is stored, retention periods and how the data is kept secure.

Data security and storage of records

Monkfield Park 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, alternatively, when this is not possible, they are logged off.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, photocopiers, pinned to notice/display boards, or left anywhere else where there is general access.
- Where staff take personal information off site, they adhere to this policy, the e-safety policy and the Internet Acceptable Use Policy.
- Passwords that are at least 8 characters long containing letters and numbers are used to access Monkfield Park computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals, and these should not be shared.
- For Ipads and for any other electronic devices which have a passcode, these should be activated.
- All devices should be set to hide notifications so that they cannot be read.
- Encryption software is used to protect all portable devices and removable media, such as laptops .
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Monkfield Park-owned equipment.
- Where Monkfield Park needs to share personal data with a third party, it carries out due diligence and takes reasonable steps to ensure it is stored securely and adequately protected.
- USB devices and external hard drives should not be used. Visitors who may bring USB devices into school must use the 'guest log on' for computers.
- If personal information is stored on a personal device and if this device is shared with others, the owner of the device must take steps to ensure that this information is not shared or accessed by a third party.

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 Monkfield Park cannot or does not need to rectify or update it.

For example, Monkfield Park will shred paper-based records, and overwrite or delete electronic files..

Personal data breaches

Monkfield Park will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, Monkfield Park will follow the procedure set out in Appendix 1.

When appropriate, Monkfield Park will report the data breach to the ICO within 72 hours. Such breaches may include, but are not limited to:

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

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 Monkfield Park's processes make it necessary.

Monitoring arrangements

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 Monkfield Park's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing body.

Privacy/fair processing notice

Privacy notice for pupils, parents/carers

Under data protection law, individuals have a right to be informed about how Monkfield Park uses any personal data that it holds about them. Monkfield Park comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where it is processing their personal data.

Monkfield Park's privacy notice explains how it collects, stores and uses personal data about **pupils** (see appendix 2).

Monkfield Park may also hold data about pupils that it has received from other organisations, including other schools, settings, local authorities and the Department for Education. Monkfield Park's record retention schedule can be found at the end of this policy (see appendix 4). The Department for Education may share information from the NPD with other organisations .

Complaints

Monkfield Park takes any complaints about its collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about Monkfield Park's data processing, please raise this with Headteacher in the first instance.

To make a complaint, please contact the Headteacher, who will liaise with the DPO.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how Monkfield Park uses any personal data that it holds about them. Monkfield Park complies with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where Monkfield Park is processing their personal data.

Monkfield Park's privacy notice explains how we collect, store and use personal data about individuals it employs, or otherwise engages, to work at Monkfield Park.

Where a member of the Monkfield Park workforce has provided Monkfield Park with consent to use their data, individuals may withdraw this consent at any time. Monkfield Park will make this clear when requesting consent, and explain how to go about withdrawing consent.

Some of the reasons for collecting and using personal information about the workforce overlap, and there may be several grounds which justify Monkfield Park's use of workforce data.

Transferring data internationally

Where Monkfield Park transfers personal data to a country or territory outside the European Economic Area, it will do so in accordance with data protection law.

Workforce members may also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact the Headteacher in the first instance, who will liaise with the DPO.

Complaints

Monkfield Park takes any complaints about collection and use of personal information very seriously.

If you think that the collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about data processing, please raise this with the Headteacher in the first instance.

To make a complaint, please contact the Headteacher in the first instance, who will liaise with the DPO.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this policy or the privacy notices in the appendices, please contact the Headteacher in the first instance, who will liaise with the DPO.

The Headteacher can be contacted at:

Monkfield Park Primary School

School Lane

Cambourne

CB23 5AX

e-mail: office@monkfieldpark.cambs.sch.uk

Tel: 01954 273377

The Data Protection Officer (DPO) can be contacted at:

Ian Hoare

dpo@theictservice.org.uk

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data at Monkfield Park.

Links with other policies

This policy may also be read in conjunction with:

Acceptable Use Code of Conduct

E-Safety

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 Headteacher
- The Headteacher in conjunction with 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 Headteacher in conjunction with 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 Headteacher in conjunction with the DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The Headteacher in conjunction with 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
    - Discrimination
    - Identify 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 Monkfield Park's computer system in a secure file on the m-drive, accessed only by authorized members of staff.
- 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 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 Headteacher in conjunction with 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 Headteacher in conjunction with 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 Headteacher in conjunction with 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 Headteacher in conjunction with 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 individuals)

  Records of all breaches will be on the Monkfield Park's computer system, stored in a secure electronic file on the m-drive, which can only be accessed only by authorized staff.

  The DPO and headteacher 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

Monkfield Park 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. Monkfield Park 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 receive personal data sent in error must alert the sender and the Headteacher as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Headteacher will ask the ICT department 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 Headteacher in conjunction with the DPO will ensure it receives a written response from all the individuals who received the data, confirming that they have complied with this request
- The Headteacher in conjunction with the DPO will carry out an internet search to check that the information has not been made public; if it has, Monkfield Park will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- Details of pupil premium interventions for named children being published on the Monkfield Park website, the Deputy Headteacher will notify the Headteacher in conjunction with the DPO
- Non-anonymised pupil exam results or staff pay information being shared with governors – the receiver must alert the clerk to the governors immediately who will recall all information and notify the Headteacher in conjunction with the DPO
- A Monkfield Park laptop containing non-encrypted sensitive personal data being stolen or hacked the Headteacher in conjunction with the DPO will notify the ICO and the police.
- Monkfield Park's cashless payment provider being hacked and parents' financial details stolen the Headteacher in conjunction with the DPO will notify the ICO.

Appendix 2

Monkfield Park Privacy Notice (How we use pupil information)

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

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical/dietary information
- Special Education Needs information
- Exclusions/behavioural information
- Personal information about a pupil's parents and/or other relatives (such as name, contact details, relationship to child)
- Relevant consent information (photographs, videos, educational visits, food tasting)

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to share data for statutory inspections and audit purposes

The lawful basis on which we use this information

We collect and use pupil information under

- The Education Act (various years)
- The Education (Pupil Registration) (England) Regulations
- The School Standards and Framework Act 1998
- The School Admissions Regulations 2012
- Children and Families Act 2014
- The Special Educational Needs and Disability Regulations 2014
- Article 6, and Article 9 (GDPR) – from 25 May 2018 (includes special category data)

The DfE process census data under the various Education Acts – further information can be found on their website: https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this.

Storing pupil data

We hold pupil data for varying lengths of time depending on what the information is.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil attend after leaving us
- our local authority (Cambridgeshire County Council) https://www.cambridgeshire.gov.uk/data-protection-and-foi/information-and-data-sharing/
- the Department for Education (DfE)
- NHS
- School nurse
- Social Care
- Cambridgeshire County Council SEND Services
- Multi Agency Safeguarding Hub (MASH)
- Early Help Hub
- CHUMS (specialist SEND services)
- CAMH (specialist mental health services)
- Statutory Assessment Team
- Locality Team
- Education Welfare Officer
- The Police Force

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

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

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

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

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

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

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

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

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact the Headteacher, Mrs Sarah Jarman on office@monkfieldpark.cambs.sch.uk or our external data protection officer e-mail dpo@theictservice.org.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at

https://ico.org.uk

Contact

If you would like to discuss anything in this privacy notice, please contact:

The Headteacher

Monkfield Park Primary School

School Lane

Great Cambourne

Cambridge

CB23 5AX

Appendix 3

Monkfield Park Privacy Notice (How we use school workforce information)

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

- personal information (such as name, employee and/ or teacher number, national insurance number, address, telephone number, e-mail address, emergency contact details)
- special categories of data including characteristics information such as gender, age, ethnic group, relevant medical information
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- safeguarding information (such as DBS/CRB/List 99 information, disqualification by association declaration)
- payroll information (such as claims forms, maternity, paternity, shared parental leave and sickness self-certification forms, discretionary leave of absence forms, study leave applications, GP Fit For Work statements and bank details).

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- inform the development of recruitment and retention policies
- enable individuals to be paid
- ensure safeguarding procedures are upheld

The lawful basis on which we process this information

We process this information under

- The Education Act (various years)
- The Education (Pupil Registration) (England) Regulations
- The School Standards and Framework Act 1998
- The School Admissions Regulations 2012
- Children and Families Act 2014
- The Special Educational Needs and Disability Regulations 2014
- Article 6, and Article 9 (GDPR) – from 25 May 2018 (includes special category data)

For regulations relating to the School Workforce Census – see the DfE website
https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you whether you are required to provide certain school workforce information to us or if you have a choice in this.

Storing this information

We hold school workforce data for employment purposes, to assist in the running of the business and/or enable individuals to be paid. In such cases we apply the 'recommended' retention period. Some personal data is retained for statutory purposes, in which case we will apply the statutory retention period. For more information please read the Personal Information Policy on the M drive.

Who we share this information with

We routinely share this information with:

- our local authority, (Cambridgeshire County Council) https://www.cambridgeshire.gov.uk/data-protection-and-foi/information-and-data-sharing/
- the Department for Education (DfE)
- EPM Ltd
- Heales Ltd (Occupational Health Service)

Why we share school workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding / expenditure and the assessment educational attainment.

EPM Ltd

We share personal data with EPM as our contracted payroll and personnel provider.

Heales Ltd

We share personal data with Heales Ltd as our contracted occupational health services provider.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative

Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

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

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

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

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

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

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

For more information about the department's data sharing process, please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

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

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Mrs Sarah Jarman, head@monkfieldpark.cambs.sch.uk or our external data protection officer dpo@theictservice.org.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

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

Further information

If you would like to discuss anything in this privacy notice, please contact:

Mrs Sarah Jarman

Monkfield Park Primary School

School Lane

Great Cambourne

Cambridge

CB23 5AX

Appendix 4

Retention guidance for Monkfield Park NB: For further, detailed information, see the Information Management Toolkit for Schools found at irms.org.uk

1. Child Protection					
	Basic file description	Data Protection Issues	Statutory Provision	Retention Period (operational)	Action at the end of the administrative life of the record.
1.1	Child Protection files	Yes	Education Act 2002, s175 related guidance "Safeguarding Children in Education", September 2004	DOB + 25 years	SECURE DISPOSAL
1.2	Allegations of Child Protection nature against a member of staff, including where the allegation is unfounded.	Yes	Employment Practices Code: Supplement Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance "Dealing with Allegation of Abuse against Teachers and Other Staff" November 2005	Until the person's retirement or 10 years from the date of allegation whichever is the longer.	SECURE DISPOSAL

2. Governors					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
2.1	Minutes				
	• Principal set (signed)	No		Permanent	
	• Confidential minutes (signed)	Yes		Permanent	
	• Inspection Copies (those available on request for the public)	No		Date of meeting + 3 years	SECURE DISPOSAL (if these minutes contain any sensitive personal information they should be shredded)
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL
2.3	Reports	No		Date of Reports + 6 years	Retain in School for 6 years from the date of meeting
2.4	Instrument of Government	No		Permanent	Retain in school whilst school is open

2.5	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
2.6	Action Plans	No		Date of Action Plan + 3 years	SECURE DISPOSAL
2.7	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 which should be kept for current year +1)
2.8	Complaints Files	Yes		Date of resolution of complaint + 6 year	Retain in school for the first six years Review for further retention in the case of contentious disputes. SECURE DISPOSAL – rountine complaints
2.9	Annual Reports required by the DfE	No	Education (Governors Annual reports) (England) (Amendment) Regulations 2002 SI2002 No 1171	Date of Report + 10 years	
2.10	Proposals for school to become, or be established as Special Status schools	No			Current year + 3 years

3. Management					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
3.1	Minutes of the Senior Management Team and other administrative bodies	Yes		Date of meeting +5 years	Retain in school for 5 years from meeting
3.2	Reports made by the Headteacher or the management team	Yes		Date of report + 3 years	Retain in school for 3 years from meeting
3.4 3	Records created by Headteachers, Deputy Headteachers, Senior Leaders and other members of staff with administrative responsibilities.	Yes		Closure of file + 6 years	SECURE DISPOSAL
3.4	Correspondence created by Headteachers,	No		Date of	SECURE DISPOSAL

	Deputy Headteachers, Senior Leaders and other members of staff with administrative responsibilities.			correspondence + 3 years	
3.5	Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
3.6	School development plans	Yes		Closure + 6 years	Review
3.7	Admissions – if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL
3.8	Admissions – if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL
3.9	Proofs of address supplied by parents as part of the admissions process	Yes		Current + 1 year	SECURE DISPOSAL
3.10	Supplementary information forms including additional information such as religion, medical conditions etc.	Yes	`	Current + 1 year	SECURE DISPOSAL

4. Pupils					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
4.1	Admission Registers	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives.
4.2	All electronic records held in SIMS (unless a child is LAC, CP or SEND)	Yes		Date of leaving + 7 years LAC, CP or SEND + 25 years	SECURE DISPOSAL
4.3	Pupil Files retained in School – Primary (including supplementary forms including additional information such as religion, medical conditions etc.	Yes		Retain for the time the pupil remains at the primary school	Transfer to 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 Pupil Referral Unit.
4.4	Special Educational Needs and Disabilities files,	Yes		DOB of the pupil +	SECURE DISPOSAL

	reviews and Individual Education Plans			25 years the review. Note : This retention period is the minimum period that any pupil file should be kept. some authorities choose to keep SEND files for a longer period of time to defend themselves in a "failure to provide a sufficient education" cases. there is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period.	
4.5	Correspondences relating to absences	No		Date of absence +2 years	SECURE DISPOSAL
4.6	Examination Results	Yes			
4.6a	• Public	No		Year of the examination + 6 Years	SECURE DISPOSAL
4.6b	• Internal examination results	Yes		Current year + 5 years	SECURE DISPOSAL
4.7	Any other record created in the course of contact with children	Yes		Current year + 3 years	Review at the end of 3 years and either allocate a further retention period or SECURE DISPOSAL.
4.8	Statement/EHCP maintained under The Education Act 1996 - section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending.
4.9	Proposed statemen/EHCP or amended statement/EHCP	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending.
4.10	Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 1	Closure + 12 years	SECURE DISPOSAL unless legal action is pending.
4.11	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 1	Closure + 12 years	SECURE DISPOSAL unless legal action is pending.
4.12	Parental permission slips for school trips - where there has been no major incidents	Yes		Conclusion of the trip	SECURE DISPOSAL

4.13	Parental permission slips for school trips - where there has been a major incidents	Yes	Limitation Act 1980	DOB of the pupil involved in the incident +25 years. The permission slips for all pupils on the trip need to be retained to show that the rules had been followed for all pupils	SECURE DISPOSAL
4.14	Records created by school to obtain approval to run an Educational Visit outside the classroom (EVOLVE)	No	3 part supplement to the Health and Safety of Pupils on Educational Visits. (HASPEV)(1998)	Date of the visit + 10 years	Safeguarding Officer Advice

5. Curriculum

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Schemes of work	No		Current year + 1 year	Review retention period or SECURE DISPOSAL
5.3	Timetable	No		Current year + 1 year	Review retention period or SECURE DISPOSAL
5.4	Class record books	No		Current year + 1 year	Review retention period or SECURE DISPOSAL
5.5	Pupils Work	No		Sent home at the end of the academic year and samples retained for Ofsted	Review retention period or SECURE DISPOSAL
5.6	SATS records - and results	Yes		Current year + 6 years	SECURE DISPOSAL
5.7	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
5.8	Self Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6. Personnel Records held in Schools

	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal Files	Yes		Termination + 7 years	SECURE DISPOSAL
6.3	Interview notes and recruitment records for successful and unsuccessful candidates	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Disciplinary proceedings	Yes	Where the warning relates to child protection see 1.2. if the disciplinary proceedings relates t a child protection matter place contact your safeguarding officers for further advice.		
6.5a	• Oral warning			Date of warning + 6 months	SECURE DISPOSAL
6.5b	• Written warning - level one			Date of warning + 6 months	SECURE DISPOSAL
6.5c	• Written warning - level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	• Final Warning			Date of warning + 18 months	SECURE DISPOSAL
6.5e	• Case not found			If child protection related please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years. In the case of serious accidents a further retention period will need to be applied	SECURE DISPOSAL
6.7	Annual Appraisal/assessment records	No		Current year + 7 years	SECURE DISPOSAL
6.8	Maternity Pay records	Yes	Statutory Maternity Pay (General) Regulation 1986 (SI 1986/1960) revised 1999 (SI1999/567)	Current year + 6 years	SECURE DISPOSAL

6.9	Records held under Retirement Benefit Scheme (Information Powers) regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
6.10	Proof of Identity collected as part of the process of checking portable enhanced DBS disclosure.	Yes		Where possible these should be checked and a note kept of what was send 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

7. 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.
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
7.2	Accident Reporting		Social Security (Claims & Payments) Regulations 1979 Regulation 25, social security Administration Act 1992 section 8 , Limitation Act 1980		
7.2a	• Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	• Children	Yes		DOB of child + 25 years	SECURE DISPOSAL
7.3	COSHH:				
7.4	Incident Reports	Yes		Current year + 20 years	SECURE DISPOSAL
7.5	Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation.			Last action + 50 years	SECURE DISPOSAL

7.9	Fire Precautions log books			Current year + 6 year	SECURE DISPOSAL

8. Administrative					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
8.1	Inventories of equipment & furniture			Current years + 6 years	SECURE DISPOSAL
8.2	School brochures or prospectus			Current years + 3 years	
8.3	Circulars (Staff/parents/pupils)			Current years + 1 year	SECURE DISPOSAL
8.4	Newsletters			Current year + 1 years	Review to see whether further retention period is required
8.5	Visitors book			Current year + 2 years	Review to see whether further retention period is required
8.6	PTA			Current year + 6 years	Review to see whether further retention period is required

9. Finance					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	
9.2	Loans and Grants		Financial regulations	Date of last payment on loan + 12 years	Review to see whether further retention period is required
9.3	Contracts				
9.3a	• under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	• under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	monitoring records			Current year + 2 years	SECURE DISPOSAL

9.4	Copy Orders			Current year + 6 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc			Current year + 6 years	SECURE DISPOSAL
9.6	Invoices, receipts and other records covered by the Financial Regulations.		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and Requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtors Records		Limitations Act 1980	Current year + 6 years	SECURE DISPOSAL

10. Property					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
10.1	Title Deeds	Yes		Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Maintenance and contractors		Financial Regulations	Current Year + 6 years	SECURE DISPOSAL
10.3	Leases			Expiry of the Lease + 6 years	SECURE DISPOSAL
10.4	Lettings			Current Year + 3 years	SECURE DISPOSAL
10.5	Burglary, theft and vandalism report forms			Current Year + 6 years	SECURE DISPOSAL
10.6	Maintenance log books			Current Year + 6 years	SECURE DISPOSAL
10.7	Contractors reports			Current Year + 6 years	SECURE DISPOSAL

11. Local Authority					
	Basic File Description	Data Protection	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the

		Issues			record.
11.1	Secondary transfer sheets (Primary)	Yes		Current years + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current years + 1 years	SECURE DISPOSAL
11.3	Circulars from LA			Whilst required operationally	Review to see whether a further retention period is required.

12. Department for Children, Schools and Families					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
12.1	HMI Reports			These do not need to be kept any longer	
12.2	OFSTED reports and papers			Replace former report with new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars form Department of Childrens schools and families			Whilst operationally required	Review to see whether a further retention period is required

13. School Meals					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
13.1	Dinner Registers			Current years + 3 years	SECURE DISPOSAL
13.2	School meals summary sheets			Current years + 3	SECURE DISPOSAL

				years	

14. Outside agencies					
	Basic File Description	Data Protection Issues	Statutory Provisions	Retention Period (operational)	Action at the end of the administrative life of the record.
14.1	Reports for outside agencies - where the report has been included on the case files created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
14.2	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
14.3	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
14.4	Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	Delete
14.5	Group Registers	Yes		Current years + 2 years	SECURE DISPOSAL