ALTRINCHAM C.E. AIDED PRIMARY SCHOOL

SCHOOL DATA PROTECTION POLICY

The Governors and Staff Altrincham C.E. Aided Primary School recognise the importance of following the principles of the General Data Protection Regulation 2018 and of making sure that information is securely and appropriately managed

The Eight Data Protection Principles

The principles state that data must be:

- Obtained and processed fairly and lawfully
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the Data Subject's rights
- Secure
- Not transferred to countries which do not have similar protective legislation

The data protection principles apply to all information held electronically, and in paper files that tell you about an identifiable living individual. Principles extend to pupils and staff records (names, date of birth, addresses, National Insurance numbers, medical records, school marks, exam results, SEN assessments, and staff development reviews.

Sensitive personal data is a separate category, such as health records, sexuality, race, religion, criminal offences, political opinions, and trade union membership where are greater responsibilities.

Processing data

As a data processor the school collects, uses, discloses, retains and disposes of information. The school registers this with the Information Commissioners Office annually.

Fair Processing

A fair processing notice is given to parents when personal information is collected, telling with whom and why you are going to share it and will do only that.

Individual Rights

The rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

The right to data portability only applies:

- to personal data an individual has provided to a controller;

where the processing is based on the individual's consent or for the performance of a contract; and

- when processing is carried out by automated means.

Provision of personal data will be in a structured commonly used and machine readable form and provide the information free of charge.

Physical Security

The school reviews the physical security of buildings, storage systems:

Paper documents are stored in locked cupboards. Never leave printed personal information on desks or noticeboards.
Electronic devices are kept secure and a log updated

Procedures are in place for data taken away from school. The staff member is responsible for the encryption of data on electronic files such as pen drives, and lap tops. Taking such measures as not to leave mark books, pupil workbooks, files, I pads, lap tops and photographs in the boot of cars etc. where they are at risk of being stolen.

Electronic Security

Data stored electronically must be secured through frequently changed passwords, and encryption software.

In the event of theft, the fines through the courts can be up to £500,000.

If the staff use their own device for school business they must be secure.

Staff leaving or the sale of the device, the school remains responsible for the data protection.

When electronic data is no longer needed it must be deleted properly.

Electronic data is stored on the Administration computer network (SIMS) and on the central server. This is password protected and access rights are restricted to authorised personnel in accordance with their job description. All confidential documents (documents containing pupils' name, DOB, address, SEN information, other personal data) must be stored on the central server on the admin or staff only folder (S, N and C drive). The data is backed up daily.

Electronic confidential data (documents containing student's name, DOB, address, SEN information, other personal data) which needs to be portable can be sent by email or shared in common drives, in the school network – however the use of email for dissemination of personal information is discouraged (see *email policy* in school). The data is always encrypted and password protected before sending/sharing. The storage of such sensitive data is not authorised on pen (USB) drives; if pen drives are to be used, independently of the sensitivity of its contents, access much be protected by password.

E-mail has become an increasingly common method of communication. Staff are urged to delete unread e-mails from unknown sources and with irrelevant subject headings in order to minimise the risks of virus transmission. Pupil data is transferred to Trafford LA, when necessary, by secure file transfer.

Subject Access Requests

Subject access requests can be made a parent on the appropriate form (available on school website) on behalf of pupils. The school must respond within 40 days.

Sharing Personal Data

The school manages what personal information to share and with whom, legitimately such as health authorities, local government, other schools, social services, and integrated services.

Information is secure when it is passed on.

The data we hold:

HOW HELD	WHAT TYPE OF SYSTEM	WHERE STORED
Manual/ Computerised SIMS & Cloud based Software	Pupils academic records	School offices/Admin computer network/ Offsite
Manual/ Computerised SIMS &SPTO	Class lists	School offices/Admin computer network/ Offsite
Manual/ Computerised SIMS	Staff Personnel files	Junior office, locked cabinet/Admin computer network/ Offsite
Computerised SIMS	Attendance records	Offsite/Admin computer network
Manual/ Computerised SIMS &SPTO	Pupil personal data	School office/Admin computer network/ Offsite
Digital Hard Drive	Security CCTV	School Admin Office.
Central Server	Photos	Digital devices, under network coverage and periodic clean up

Retention of Data

See Appendix: Records Management Policy

Review date……

Chair of Governors…….signature

Head teacher……signature

- **Appendix 1 School Privacy Notice**
- **Appendix 2 Subject Access Form**
- **Appendix 3 Privacy Impact Assessment**
- **Appendix 4 School Data Breach Procedure**
- **Appendix 5 CCTV Surveillance**
- **Appendix 6 Records Management Policy**

APPENDIX 1

ALTRINCHAM C.E. AIDED PRIMARY SCHOOL

PRIVACY NOTICE

How we use pupil information

Altrincham C.E. aided Primary School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to pupils and their families is to be processed. Samantha Tanney acts the school data protection officer, and can be contacted on 0161 9287288 or altrinchamce.admin@trafford.gov.uk.

We collect and hold personal information relating to our pupils and may also receive information about them from their previous school, local authority and/or the Department for Education (DfE). We use this personal data to:

- support our pupils' learning
- monitor and report on their progress
- provide appropriate pastoral care; and
- assess the quality of our services
- protect public monies against fraud
- to safeguard pupils

This information will include their contact details, national curriculum assessment results, attendance information, any exclusion information, where they go after they leave us and personal characteristics such as their ethnic group, any special educational needs they may have as well as relevant medical information.

Why do we collect and use your information

Altrincham C.E. Aided Primary School holds the legal right to collect and use personal data relating to pupils and their families, and we may also receive information regarding them from previous school, LA and/or the DfE. We collect and use personal data in order to meet legal requirements and legitimate interests set out in the GDPR and UK Law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR 2018
- Education Act 1996
- Regulation 5 of the Education (Information About Individual Pupils) (England) regulations 2013.

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

- personal information (such as name, date of birth and address)
- characteristics (such as gender, ethnicity and disability)
- information relating to episodes of being a child in need (such as referral information, assessment information, Section 47 information, Initial Child Protection information and Child Protection Plan information)
- episodes of being looked after (such as important dates, information on placements)
- information relating to referrals under Educational Health Care Plan, SEND, SARF, CHAMS and Behavioural Support Plans,
- outcomes for looked after children (such as whether health and dental assessments are up to date, strengths and difficulties questionnaire scores and offending)
- adoptions (such as dates of key court orders and decisions)

A parent/guardian can request that only their child's name, address and date of birth be passed to Trafford Local Authority by informing: School Office Manager- Mrs Helen Dunn 0161 928 7288.

To ensure your son or daughter's information is kept safe we have the following controls/limitations in place:

a) the information will not be used for any purpose other than those stated in this notice
b) the information will be held within secure systems/locations, with appropriate levels of security, that comply with relevant data protection legislation
c) the information will only be shared for lawful purposes and with an appropriate level of security that complies with relevant data protection legislation
d) the information will only be held for the periods agreed in our school's Record Retention Policy and Schedule, after which it will be destroyed. Our School's Record Retention and Schedule can be found in school policies.

e) the information will be held, used and shared in accordance with Data Protection Act 1998 legislation and the General Data Protection Regulation (GDPR) which comes into force on 25 May 2018.

Who we share this information with

We routinely share this information with:

- The Department for Education (DfE)
- Trafford CYPS
- Pennine Care Trust NHS
- Schools – transfer of pupils

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about children in England. It provides invaluable information on the background and circumstances on a child's journey and 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 children to the DfE as part of statutory data collections. Some of this information is then stored in the national pupil database (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

We will not give information about our pupils to anyone without your consent unless the law and our policies allow us to do so. When you give your consent for your son or daughter's information to be held and/or shared for any purpose you can withdraw that consent at any time by contacting:

- School Office Manager- Mrs Helen Dunn 0161928 7288.

You can also contact the person named above if you wish to:

- access any records we hold about your son or daughter
- have any information we hold about your son or daughter corrected
- have any information we hold about your son or daughter erased
- restrict how information we hold about your son or daughter can be used or shared
- object to information about your son or daughter being held
- have any information we hold about your son or daughter transferred to a third party
- challenge decisions relating to your son or daughter made using automated decision making and profiling

We are required, by law, to pass certain information about our pupils to our local authority (LA) and the Department for Education (DfE).

Department for Education (DfE) - We share children in need and children looked after data with the Department on a statutory basis, under Section 83 of 1989 Children's Act, Section 7 of the Young People's Act 2008 and also under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.
This data sharing helps to develop national policies, manage local authority performance, administer and allocate funding and identify and encourage good practice.

We do not share information about our children in need or children looked after with anyone without consent unless the law and our policies allow us to do so.

DfE may also share pupil level personal data that we supply to them, with third parties. This will only take place where legislation allows it to do so and it is in compliance with the General Data Protection regulation 2018.

Decisions on whether DfE releases this personal data to third parties are subject to a robust approval process and are 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 level data, requestors must comply with strict terms and conditions covering the confidentiality and handling of data, security arrangements and retention and use of the data.

For more information on how this sharing process works, please visit: https://www.gov.uk/guidance/national-pupil-database-apply-for-a-data-extract

For information on which third party organisations (and for which project) pupil level data has been provided to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received

If you need more information about how our local authority and/or DfE collect and use your information, please visit:

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

If you are unable to access these websites, please contact:

For DfE:

Public Communications Unit,
Department for Education,
Sanctuary Buildings,
Great Smith Street,
London, SW1P 3BT
Website: www.education.gov.uk
Email: http://www.education.gov.uk
Telephone: 0370 000 2288

Should you have any concerns or complaints relating to your son or daughter about how we, as a school, obtain, use, store or share their personal data please contact:

- School Office Manager- Mrs Helen Dunn 0161928 7288.

If however you are dissatisfied with our response to your concerns you can of course contact the:

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number
Fax: 01625 524 510
Website: https://ico.org.uk/

* The Information Commissioners Office deals with concerns and complaints relating to data protection and freedom of information legislation.

Appendix 2

ALTRINCHAM C.E AIDED PRIMARY SCHOOL

Request Form for Subject Access to School Files

Request for Access to Personal Data

Under the General Data Protection Regulation 2018, you have the right to enquire of any organization whether they hold your personal data and to see a copy of that data. Individuals are called 'data subjects' in the Act.

If you require copies of data we may hold, please complete all sections below and return this form together with the necessary verification details. The information on the form will only be used to process your request and find information which relates to you. It will be kept on file to respond to any subsequent correspondence, and will not be used for any other purpose. A response will be provided within one month of receipt of the completed form and proof of identity.

Governance – Data Requests Charges

The general charge for photocopying, printing and faxing or emailing information as an attachment is £0.10 per sheet. Postage charges will be at the appropriate rate. For more substantial items, the fee charged depends on whether it is estimated that it would cost more or less than £450.00 to provide the information.

In the vast majority of cases the cost will be under £450.00 the charge will only be for photocopying, printing, faxing and postage. There may also be a charge for any work required to put the information into the required format, which could involve, for example:

- summarising the information;
- putting the information onto CD, video or audio cassette, or;
- translating the information into a different language.

Charges would not normally be made for providing information in an alternative format where this is requested on grounds of disability.

1. Details of Person Requesting Information		
Full Name:		
Date of Birth:		
Address:		
Tel. No.	**Fax No.**	**E-Mail**

Other Address Details (if less than 3 years at above address)

4. Are You the Data Subject?

YES: If you are the Data Subject please supply evidence of your identity – passport, driving licence or birth certificate (**originals only**) sent by special delivery unless you are able to bring them in person. Documents will be returned by special delivery. (Please go to question 7.)

NO: **Are you acting on behalf of the Data Subject with their written authority? If so, that authority must be enclosed. (Please complete questions 5 and 6)**

5. Details of the Data Subject (if different to 1.)
Full name
Date of Birth
Address

Tel. No. **Fax No.** **E-Mail**

6. Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf.

7. Please describe the information you require:

8. Please add any additional details (such as relevant dates, contact names, references etc.)

9. Does the information requested include information relating to another person (a 3rd party)? YES/NO
10. Do you wish to view the information in person? YES/NO (information will otherwise be supplied in hard copy to the address supplied above)
Signed **Date**

Please note that it may be necessary to seek further information or proof of identity (of data subject or agent) before the request can be processed. If this is the case, then the statutory one month limit on response will start from the date that the School receives all necessary information and proof. Every effort will be made to provide you with access or send you your details (along with an explanation of any codes or technical terms used) as soon as possible after receipt of your application.

If there is any part of this form you do not understand, or if you need further guidance, please contact the School.

Please return the completed form to the School. The following documents must accompany this application:

- evidence of your identity;
- evidence of the data subject's identity (if different from above) and their authority.

Appendix 3

ALTRINCHAM C.E. AIDED PRIMARY SCHOOL

Privacy Impact Assessment Procedures

Important Note

This procedure document has been produced based on current General Data Protection Regulations (GDPR) information.

Privacy Impact Assessment Procedure for [Insert name of school]

The following privacy impact assessment procedure been written to be included as an Annex/ Appendix to the School's Data Protection Policy.

1. Introduction

A privacy impact assessment (PIA) is a tool which can help Altrincham C.E. Aided Primary School identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow Altrincham C.E. Aided Primary School to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This procedure explains the principles which form the basis for a PIA.

The main body of the procedure sets out the basic steps which the School should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a PIA should be used throughout the development and implementation of the School's project.

A PIA will enable the School to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs should be applied to all new projects, because this allows greater scope for influencing how the project will be implemented. A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the School needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising. A PIA should be undertaken before a project is underway.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone.

It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.

- **Informational privacy** – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It

can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

.

5. Informational Privacy

This procedure is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Whilst a PIA is not a legal requirement (except 'high risk processing i.e. safeguarding data), the ICO may often ask an organisation whether they have

carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within the School and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.
- A data sharing initiative where two or more schools seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of the school.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications.
- The collection of new data on an existing system.

7. PIA Procedure

The format for an initial PIA is at **Annex A.**

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at **Annex B**

The links between the PIA and DPA are set out in **Annex C**

8. Monitoring

The completed PIA should be submitted to the Governing Body for review and approval. The Governing Body will monitor implementation of actions identified in PIA's

(Extracted from the ICO – PIA Code of Practice)

Annex A

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
- Will the project require you to contact individuals in ways that they may find intrusive?

(Extracted from the ICO – PIA Code of Practice)

Annex B

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex C can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Extracted from the ICO – PIA Code of Practice

Annex C

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Appendix 4

Altrincham C.E. Aided Primary School Data Breach Procedure

Important Note

This procedure has been produced based on current General Data Protection Regulations (GDPR) information. As further updates are released this procedure may be updated to reflect the changes.

The GDPR will apply in the UK from 25 May 2018

Data Breach Procedure for Altrincham C.E. Aided Primary School

The School data breach procedure has been written to be included as an Annex/Appendix to the School's Data Protection Policy.

Policy Statement

Altrincham C.E. Aided Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by Altrincham C.E. Aided Primary School and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at Altrincham C.E. Aided Primary School if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

The school data protection officer is Mrs Samantha Tanney (0161 928 7288, altrinchamce.admin@trafford.gov.uk)

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant Trafford Local Authority and Chester Diocesan Board l Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

c. Contacting the Trafford LA Media Office (Legal) if part of the crisis service, so that they can be prepared to handle any press enquiries.

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and

Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Chair of School Governors…….date

Head teacher……....date

Appendix 5

ALTRINCHAM C.E AIDED PRIMARY SCHOOL

CCTV Surveillance

The school uses CCTV surveillance to safeguard pupils, and as such is the data controller. Cameras are located above key exit/ entry points of the main building.

Individuals are made aware they may be recorded through signage. Images are kept secure and access is restricted and a log kept.

Recorded images (mostly at a distance) are stored on a password protected hard drive and kept for 30 days before removal.

Recorded images are viewed in a restricted office location.

Disclosure requests are handled where the head/ deputy have clear guidance on the circumstances in which it is appropriate to make a disclosure or not.

CCTV images are recorded solely for security and not pupil behaviour management.

The head/ deputy to consider on a disclosure request as to whether identifying features of any other individuals can be obscured. The school has the discretion to refuse any request for information unless there is an overriding legal obligation.

Further advice can be found: ICO website ‘A data protection code of practice, surveillance cameras.’

Appendix 6

ALTRINCHAM C.E. AIDED PRIMARY SCHOOL

RECORDS MANAGEMENT POLICY

1 Introduction

The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This document provides the policy framework through which this effective management can be achieved and audited.

2 Scope of the Policy

2.1 This policy applies to all records that are created, received or maintained by staff of the school in the course of carrying out its functions.

2.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.

2.3 A small percentage of the school's records may be selected for permanent preservation as part of the institution's archives and for historical research.

3 Responsibilities

3.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Head of the School.

3.2 The person responsible for records management in the school will give guidance about good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

3.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

Recording Systems

Information created by the school must be managed against the same standards regardless of the media in which it is stored.

4.1 Maintenance of Record Keeping Systems

i. It is important that filing information is properly resourced and is carried out on a regular basis. It is equally important that the files are edited of extraneous information where appropriate on a regular basis. Removing information from a file once a freedom of information request has been made will be a criminal offence (unless it is part of normal processing).

ii. Applying retention periods is straightforward provided files are closed on a regular basis.

iii. Once a file has been closed, it should be moved out of the current filing system and stored either in a record room in the school or in another appropriate place until it has reached the end of the retention period.

iv. Information security is very important especially when dealing with personal information or sensitive policy information. There are a number of basic rules:

All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended;

Personal information held on computer systems should be adequately password protected.

Information should never be left up on a screen if the computer is unattended;

Files containing personal or sensitive information should not be left out on desks over night;

Where possible sensitive personal information should not be sent by e-mail;

If files need to be taken off the premises they should be secured in the boot of a car or in lockable containers;

Teachers may carry data on memory sticks or other removable data carriers in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software.

All computer information should be backed up regularly and the back-up should be stored off the site.

Information contained in email, fax should be filed into the appropriate electronic or manual filing system once it has been dealt with.

4 The Safe Disposal of Information Using the Retention Schedule

4.1 Files should be disposed of in line with the attached retention schedule (see appendix). This is a process which should be undertaken on an annual basis during the month of August.

4.2 Paper records containing personal information should be shredded using a cross-cutting shredder. Other files can be bundled up and put in a skip or disposed of to the waste paper merchant. Loose papers should not be put in skips unless the skip has a lid. CD's/DVD's/Floppy disks should be cut into pieces. Audio/Video tapes and fax rolls should be dismantled and shredded.

4.3 Electronic data should be archived on electronic media and 'deleted' appropriately at the end of the retention period.

Retention Schedule

Child Protection

The retention and use of records relating to child protection matters concerning pupils, and child protection allegations against staff requires specific guidance in this schedule.

Basic File Description	Data Prot	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Child Protection files	Yes	Education Act 2002, s175, related guidance 'Safeguarding Children in Education',	DOB + 25 years [1]	SECURE DISPOSAL
Allegation of a child protection nature against a member of staff, including where the allegation is unfounded	Yes	Employment Practices Code: Supplementary Guidance 2.13.1 (Records of Disciplinary and Grievance) Education Act 2002 guidance 'Dealing with	Until the person's normal retirement age, or 10 years from the date of the allegation if that is longer	SECURE DISPOSAL

Governors

Basic File Description	Data Prot	Statutory Provisions	Retention Period	Action at the end of the administrative life of the record
Minutes				
Principal set (signed)	No		Permanent	Retain in school for 6 years from date of meeting
Inspection Copies	No		Date of meeting + 3 years	SECURE DISPOSAL [If these minutes contain any sensitive personal information they must be shredded]
Agendas	No		Date of meeting	SECURE DISPOSAL
Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
Annual Parents' meeting papers	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
Instruments of Government	No		Permanent	Retain in school whilst school is open
Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
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)
Complaints files	Yes		Date of resolution of complaint + 6 years	Retain in school for the first six years. Review for further retention in the case of contentious disputes. SECURE DISPOSAL routine complaints
Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.S1 2002 No	Date of report + 10 years	

Management

Basic File Description	Data Prot	Statutory Provisions	Retention Period [operational]	Action at the end of the administrative life of the record
Log Books [Books where the Headteacher or another member of staff keeps a record of what happens in the school, this may include details of events, photographs and other information]	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
Minutes of the Senior Management Team and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
Reports made by the headteacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities.	Yes		Closure of file + 6 years	SECURE DISPOSAL
Correspondence created by headteachers, deputy headteachers, heads of year **and other members of staff with**	No		Date of correspondence + 3 years	SECURE DISPOSAL
Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
School Development Plans	Yes		Closure + 6 years	Review

Pupils				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Admission Registers	Yes		Date of last entry in the book (or file) + 6 years	Retain in the school for 6 years from the date of the last entry then consider transfer to the archives.
Attendance registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]
Pupil record cards	Yes			
Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school)
Pupil files	Yes			
Primary			Retain for the time which the pupil remains at the primary school	Transfer to the Secondary school (or other primary school)
Special Educational Needs files, reviews and Individual Education Plans	Yes		DOB of the pupil + 25 years then review. NOTE: This retention period is the minimum period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the	SECURE DISPOSAL
Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL
Examination results	Yes			
Public	No		Year of examinations + 6 years	SECURE DISPOSAL
Internal examination results	Yes		Current year + 5 years [(2)]	SECURE DISPOSAL
Any other records created in the course of contact with pupils	Yes/No		Current year + 3 years	Review at the end of 3 years and either allocated a further retention period or SECURE DISPOSAL
Statement maintained under The Education Act – Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 30 years	SECURE DISPOSAL unless legal action is pending

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

Pupils cont'd.				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Proposed statement or amended statement	Yes	Special Educational Needs and	DOB + 30 years	SECURE DISPOSAL unless legal action is pending
Advice and information to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Accessibility Strategy	Yes	Special Educational Needs and	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
Parental permission slips for school trips – where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
Parental permission slips for school trips – where there has been a major incident	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

Curriculum				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
Schemes of work	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
Timetable	No		Current year + 1 year	SECURE DISPOSAL
Class record books	No		Current year + 1 year	SECURE DISPOSAL
Mark Books	No		Current year + 1 year	SECURE DISPOSAL
Record of Homework set	No		Current year + 1 year	SECURE DISPOSAL
Samples of Pupils work	No		Current year + 1 year	SECURE DISPOSAL
Examination results	Yes		Current year + 6 years	SECURE DISPOSAL
SATS records – Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
Value Added & Contextual	Yes		Current year + 6 years	SECURE DISPOSAL
Self-Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

Personnel				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL
Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
Pre-employment vetting information (including unsuccessful DBS checks)	No	DBS guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]
Disciplinary proceedings	Yes	Where the warning relates to child protection issues see 1.2. If the disciplinary proceedings relate to a child protection matter please contact your safeguarding children officer for further advice.		
Oral warning			Date of warning + 6 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
Written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
Written warming – level 2			Date of warning + 12 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
Final warning			Date of warning + 18 months	SECURE DISPOSAL If this is placed on a personal file, it must be weeded from the file
Case not found			If child protection related please see 1.2, otherwise SECURE DISPOSAL immediately at the conclusion of the case	
Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents a further retention	SECURE DISPOSAL
Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
Maternity pay records	Yes	Statutory Maternity Pay (General Regulations1986 (SI 1986/1990), revised 1999 (SI 1999/567)	Current year + 3 years	SECURE DISPOSAL
Records held under **Retirement**	Yes		Current year + 6 years	SECURE DISPOSAL
Proofs 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 seen and what has been checked. If it is felt necessary to keep copy documentation then this should be placed on the	

Health and Safety				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL
Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security		
Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
Children	Yes		DOB of child + 25 years [3]	SECURE DISPOSAL
COSHH			Current year + 10 years [Where appropriate an additional retention period may be allocated]	
Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have come in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL
Fire Precautions log books			Current year + 6 years	SECURE DISPOSAL

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

Administrative				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Employer's Liability			Closure of the school + 40 years	SECURE DISPOSAL
Inventories of equipment and furniture			Current year + 6 years	SECURE DISPOSAL
General file series			Current year + 5 years	Review to see whether a further retention period is required
School brochure/prospectus			Current year + 3 years	Transfer to Archives [The appropriate archivist will then take a sample for permanent preservation]
Circulars			Current year + 1 year	SECURE DISPOSAL
Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
Visitors' book			Current year + 2 years	Review to see whether a further retention period is required
PTA/Old Pupils' Associations			Current year + 6 years	Review to see whether a further retention period is required

Finance				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Annual Accounts		Financial Regulations	Current year + 6 years	Archive
Loans and grants		Financial regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
Contracts				
Under seal			Contract completion date + 12 years	SECURE DISPOSAL
Under signature			Contract completion date + 6 years	SECURE DISPOSAL
Monitoring records			Current year + 2 years	SECURE DISPOSAL
Copy orders			Current year + 2 years	SECURE DISPOSAL
Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL

Finance cont'd.				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
School Fund – Cheque books			Current year + 3 years	SECURE DISPOSAL
School Fund – Paying in books			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Ledger			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Invoices			Current year + 6 years then review	SECURE DISPOSAL
School Fund – Receipts			Current year + 6 years	SECURE DISPOSAL
School Fund – Bank statements			Current year + 6 years then review	SECURE DISPOSAL
School Fund – School			Current year + 6 years then review	SECURE DISPOSAL
Student grant applications			Current year + 3 years	SECURE DISPOSAL
Petty cash books		Financial Regulations	Current year + 6 years	SECURE DISPOSAL

Property				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the administrative life of the record**
Title Deeds			Permanent	These should follow the property unless the property has been registered at the Land Registry
Plans			Permanent	Retain in school whilst operational
Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
Leases			Expiry of lease + 6 years	SECURE DISPOSAL
Lettings			Current year + 3 years	SECURE DISPOSAL
Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
Maintenance log books			Current year + 6 years	SECURE DISPOSAL
Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

Department for Education				
Basic File Description	**Data Prot**	**Statutory Provisions**	**Retention period [operational]**	**Action at the end of the administrative life of the record**
HMI reports			These do not need to be kept any longer	
OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
ISI reports and paper			Replace former report with any new inspection report	Review to see whether a further retention period is required
Returns			Current year + 6 years	SECURE DISPOSAL
Circulars from DFE			Whilst operationally required	Review to see whether a further retention period is required

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

5 Monitoring and Review

This policy has been reviewed and approved by the head teacher and school governors. The Records Management Policy will be reviewed and updated as necessary every 2 years.