Information Systems Policy

Aim of the Langley Academy Trust

To provide an outstanding education for every child in the trust through high aspirations and through the principles of quality learning using curiosity, exploration and discovery.

The information systems policy covers the use of the Trust's computer systems (hardware, software, data, telephone network, computer network, email and internet) by all staff, and the use of online tools provided by the Trust. This policy consists of three sections:

1. Acceptable use of ICT equipment

2. Use of telephones, email and internet by staff

3. Safe use of online resources

This policy is linked to:

- Staff Discipline Policy
- E-safety Policy
- Staff Code of Conduct Policy
- Data Protection Policy
- GDPR Privacy Statement for Employees

1. **Acceptable use of Computer Systems: Principles**

The Trust is committed to safeguarding its computing system to ensure it can be used in the most effective manner to support the teaching and learning processes and enable The Trust's business tasks to be undertaken. Ensuring the safety and integrity of the Trust's ICT system is the responsibility of all staff.

The Trust encourages staff to fully use the computing infrastructure and to make use of Mobile Computer Devices equipment offsite to support them in their work. The Trust encourages this use in a responsible and professional manner. Mobile devices include for example laptops, tablets, notebooks, smartphones and other portable/mobile devices.

As a user of the Trust's Computer systems you have a right to use it responsibly. These user responsibilities are outlined below. Misusing the Trust's computing systems may breach this and other Trust policies.

Ignorance of this policy and the responsibilities it places on you, is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.

Staff are advised of this policy during their induction and of the Trust's requirement for them to adhere to the conditions therein.

For the purposes of this policy the term "computing services" refers to any computing resource made available to you, any of the network borne services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own device to the Trust's network and the services available are particularly reminded that such use requires compliance to this policy.

Purposes

• To protect the Trust's networks and equipment

• To protect the Trust's data

• To protect the Trust and its employees from activities that might expose them to legal action from other parties

Guidelines

Password security

Access to all systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the Trust.

Issuance and continued use of your User Account is conditional on your compliance with this policy.

User ID's and passwords must not be shared or revealed to any other party. Staff must assume personal responsibility for usernames and passwords for all accounts and sites connected with their employment at the Trust. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy.

Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords are set by policy to expire every 3 months so users are forced to change their passwords. Passwords should be changed immediately if the user believes or suspects that their account has been compromised.

General Conditions

In general, use of Trust "computing services" should be for your/the user's study, research, teaching or the administrative purposes of the Trust. Some use of the facilities and services for personal use is accepted, so long as such activity does not contravene the conditions of this policy.

• Your use of the Trust's computing services must at all times comply with the law.

• Your use of the Trust's computing services must not interfere with any others' use of these facilities and services.

• You are not entitled to use a computer/device that you have not been authorised to use.

• You must not access any program or data which has not been specifically authorised for your use.

• You must not use or copy any data or program belonging to other users without their express and specific permission.

• You must not alter computer material belonging to another user without the user's permission.

• You must not use Trust computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.

• You must not use Trust computing services for the creation, modification, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Headteacher).

• You must not use the Trust's computing services to conduct any form of commercial activity without express permission.

• You must not use the Trust's computing services to disseminate mass (unsolicited) mailings.

• You must not install, use or distribute software for which you do not have a license, and which is not first authorised by the ICT technicians for installation

• You must not use any P2P/torrent client as these enable illegal sharing of copyrighted material

• You must not use any IRC or messenger software including, but not limited to WhatsApp, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorised to do so for work related purposes

You must not use any Messenger Software, including but not limited to WhatsApp, Hangouts, Internet Relay Chat (IRC), unless authorised to do so from the Principal for work related purposes.

• You must not post or subscribe to newsgroups, on-line discussion boards or email list groups from the Trust facilities, unless specifically related to Trust activities

• You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Executive Principal/Governing Board

• You must not play computer games of any nature whether preinstalled with the operating system or available online unless it has been agreed by your line manager as having educational value for children or it is outside of your working hours

Data Security

The Trust holds a variety of sensitive data including personal information about students/pupils and staff. If you have been given access to this information, you are reminded of your responsibilities under the Data Protection Act 2018 and General Data Protection Regulations 2018 (GDPR).

You should only take a hard copy of data outside the Trust's systems if absolutely necessary, and you should exhaust all other options before doing so. This includes putting sensitive data onto laptops, any removable encrypted storage device, and cloud storage or into secure emails, also personal cloud storage solutions (example: MS OneDrive, Google drive, iCloud) for the transfer of Trust information is expressly forbidden. Use of cloud storage must be authorised by the Data Protection Officer. If you do need to take data outside the Trust, this should only be with the authorisation of the Trust's Data Protection Officer. As part of this you should perform a risk assessment on the implications of it falling into the wrong hands, and take appropriate steps to mitigate against this. This will almost certainly include encrypting the information, and checking the data protection statements of any recipients of the data.

There are a variety of methods of remote access to systems available (in particular using VPN and remote desktop or terminal services) which allow you to work on data in-situ rather than taking it outside the Trust, and these should always be used in preference to taking data off-site.

The ICT Technicians offers a variety of information and support to help you keep data secure. If you are uncertain about any aspect of data security, you must contact them for advice.

Anti-Virus and Firewall Security

All Trust devices are installed with current versions of virus protection and firewall software by the ICT Technicians. Users cannot alter the configuration of this software and no attempt should be made to do so by any means. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files.

Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the ICT Technicians immediately. If the ICT Technicians detects a machine behaving abnormally due to a possible viral infection it will disconnected from the network until deemed safe.

Physical Security

The users of computing equipment should always adhere to the following guidelines:

• Treat equipment safely, in the same manner as a reasonable person would

• Keep liquids away from ICT equipment

• Do not place heavy objects on ICT equipment

• Do not drop ICT equipment or objects onto it

• Any portable computer must be securely locked away when not in use

• Portable computer security is your responsibility at all times

• Do not leave the portable computer unattended in a public place or within the Trust

• Do not leave the portable computer inside your car

• Extra reasonable care must be taken to prevent the loss of any removable storage device which contain confidential Trust data

• Staff supervising students using ICT equipment should ensure students take reasonable care of such equipment

Remote Access

Remote access to the Trust network is possible where this has been granted by the ICT Technicians.

Remote connections are considered direct connections to the Trust network. As such, generally accessing services remotely, subjects the user to the same conditions, requirements and responsibilities of this policy.

All connection attempts are logged.

Monitoring and Logging

Activities regarding network transactions may be monitored and logged and kept for an appropriate amount of time. Logs are taken for reasons of security, diagnostic and account/audit reasons. Logs are available to the Network Manager and ICT Technicians and kept for no longer than necessary and in line with current data retention schedule.

Such records and information are sometimes required - under law - by external agencies and authorities. The Trust will comply with such requests when formally submitted.

Breaches of this Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence.

It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

In the event a Portable Computer/ Mobile Device is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the Trust.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

• Taking food and/or drink into rooms with computing facilities where they are forbidden

• Sending nuisance (non-offensive) email

• Behaving in a disruptive manner

Not all first offences will automatically be categorised at this level since some may be of a significance or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

• Repeated minor breaches within the above detailed 12-month period

• Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area

• Assisting or encouraging unauthorised access

• Sending abusive, harassing, offensive or intimidating email

• Maligning, defaming, slandering or libelling another person

• Misuse of software or software license infringement

• Copyright infringement

• Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include but are not limited to:

• Repeated moderate breaches

• Theft, vandalism or willful damage of/to Computing facilities, services and resources

• Forging email i.e. masquerading as another person

• Loading, viewing, storing or distributing pornographic or other offensive material

• Unauthorised copying, storage or distribution of software

• Any action, whilst using Trust computing services and facilities deemed likely to bring the Trust into disrepute

• Attempting unauthorised access to a remote system

• Attempting to jeopardise, damage circumvent or destroy Computing systems security

• Attempting to modify, damage or destroy another authorised users data

• Hacking into the Trust's network infrastructure to disrupt network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by Leadership under the direction of the Headteacher/Executive Principal. That investigative report will be passed to the staff member's Line Manager, to be considered within the Trust's disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

2. Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the internet on a device. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This Policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the Internet.

The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure.

This Policy has been designed to safeguard the legal rights of members of staff under the terms of the Data Protection Act, GDPR and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of Trust telephones, email and internet facilities.

To clarify when the Trust may monitor staff usage of these facilities.

Guidelines

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on Trust telephones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

The use of Trust telephones for private purposes, which are unreasonably excessive or for Trust purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the Trust reserves the right to record calls.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication.

Employees should be careful that before they open any attachment to an e-mail they receive, they are reasonably confident that the content is in no sense obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the Trust. Any other use of e-mail for either personal or Trust purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

Where the Trust has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address.

The Trust also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their Trust role. However, it is legitimate for employees to make use of the Internet in its various forms in the same way as email above as long as

it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene.

Unauthorised use of the Internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. The Trust reserves the right to audit the use of the Internet from particular Personal Computers/devices or accounts where it suspects misuse of the facility

Use of personal devices

Where staff use their own personal equipment such as mobile telephones, laptops, notebooks, tablets etc, if they are on Trust premises, or being used to access Trust data from anywhere, this must be with the permission of the Trust and the devices must be secure with confidential passwords.

Monitoring the use of telephone, e-mail and the Internet

It is not the Trust's policy, as a matter of routine, to monitor an employee's use of e-mail service or of the Internet via the Trust's networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Executive Principal or Governing Board may grant permission for the auditing of an employee's telephone calls e-mail or the Internet. Once approved, the monitoring process will be undertaken by designated staff acting, for operational purposes, under the direction of the Headteacher/Executive Principal.

These individuals are required to observe the strictest confidentiality when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case. They will make their reports directly to the Executive Principal/Governing Body or their delegated representative to enable Human Resources to advise the appropriate line manager/head of faculty the actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

3. Safe use of Management Information Systems

Principles

This applies wherever access to the Trust Management Information Systems (MIS) are provided. This applies to all online resources provided by the Trust, for example Capita SIMS. This policy applies whenever information is accessed through the Trust MIS, whether the computer equipment used is owned by the Trust or not. The policy applies to all those who make use of the Trust's MIS resources.

Purposes

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of the Trust's data, the Authorised MIS User and the individuals to which the MIS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials
- The wrongful disclosure of private, sensitive, and confidential information
- Exposure of the Trust to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the Data Protection Act (2018) and GDPR (2018) are adhered to.

This Policy aims to promote best use of the MIS system to further the communication and freedom of information between the Trust and Parents/Carers.

Guidelines

The Trust's MIS system is provided for use only by persons who are legally responsible for student(s)/pupils currently attending the Trust. Access is granted only on condition that the individual formally agrees to the terms of this Policy.

The authorising member of Trust staff must confirm that there is a legitimate entitlement to access information for students/pupils the names of whom must be stated on the Online Usage Policy Declaration.

A copy of the form will be held by the Trust for audit purposes.

Personal Use

Information made available through the MIS system is confidential and protected by law under the

Data Protection Act 2018, and GDPR. To that aim:

Users must not distribute or disclose any information obtained from the MIS to any person(s) with the exception of the student/pupil to which the information relates or to other adults with parental/carer responsibility.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Questions, Complaints and Appeals

MIS users should address any complaints and enquiries about the MIS system to the Trust in writing to the Network Manager and Executive Principal.

The Trust reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

• The validity of parental/carer responsibility is questioned

• Court ruling preventing access to child or family members is issued

• Users found to be in breach of this policy

If any child protection concerns are raised or disputes occur the Trust will revoke access for all parties concerned pending investigation.

Please note: Where MIS access is not available the Trust will still make information available according to the Data Protection Act (1998) and GDPR. For more information relating to data retention please see Appendix 1 – Data Retention Schedule

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Upon leaving the Trust, members of staff must return all equipment and information, including equipment and data on or before the agreed leaving date (eg last day of employment) to their Line Manager or other Academy representative. This includes, but is not limited to:

All information, including data, used or stored as part of the role, both physical and electronic.

All information, including files, documents and emails, including any data stored within individual accounts

Access control and ID cards

After leaving members of staff may not attempt to access or use any Academy information, including any data.

The Langley Academy Trust

Computing Services Declaration

Please only sign if you have fully read this Information Systems policy. By signing the declaration form you are agreeing that you have fully understood the terms and conditions and all the instructions/policies of the Trust Computing Services.

Please contact the Trust Network Manager if you are not sure of any policies and terms and conditions of use.

Declaration

I hereby confirm that I have read and fully understood the terms and conditions document attached and will strictly follow the policies of the Langley Academy Trust Computing Services

Signature……..

Staff/Governor/Trustee/Volunteers Name……..

Parent/Carer Name……

Child(ren) Name(s)……Year /Class)……..

Child(ren) Name(s)……Year /Class)……..

Child(ren) Name(s)……Year /Class)……..

Date……

Review Date: June 2019

Ratified Date: June 2019

Author: Rhodri Bryant

Date of next review: June 2022

Appendix 1: Data Retention Schedule

Management of the School 1.1 Governing Body

Basic File Description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
1.1.1 Agendas for Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to		One copy should be retained with the master set of minutes. All other copies can be disposed of	SECURE DISPOSAL (1)
1.1.2 Minutes of Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to			
Principal Set (signed)			PERMANENT	If the school is unable to store these then they should be offered to the County Archives Service
Inspection Copies (2)			Date of meeting + 3 years	If these minutes contain any sensitive, personal information they
1.1.3 Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to		Reports should be kept for a minimum of 6 years. However, if the minutes refer directly to individual reports then the reports should be kept permanently	SECURE DISPOSAL or retain with the signed set of the minutes
1.1.4 Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002	No	Education Act 2002, Section 33	Date of the meeting + a minimum of 6 years	SECURE DISPOSAL
1.1.5 Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.6 Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
1.1.7 Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.8 Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.9 Records relating to complaints dealt with by the Governing Body	Yes		Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes	SECURE DISPOSAL

1.1.10 Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002	No	Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002 SI 2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.11 Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies	No		Date proposal accepted or declined + 3 years	SECURE DISPOSAL
1.2 Head Teacher and Senior Management Team				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.2.1 Log books of activity in the school maintained by the Head Teacher	There may be data protection issues if the log book refers to individual pupils		Date of last entry in the book + a minimum of 6 years then review	These could be of permanent historical value and should be offered to the County Archives Service if appropriate
1.2.2 Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3 Reports created by the Head Teacher or the Management Team	There may be data protection issues if the report refers to individual pupils		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4 Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5 Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils		Date of correspondence + 3 years then review	SECURE DISPOSAL
1.2.6 Professional Development Plans	Yes		Life of the plan + 6 years	SECURE DISPOSAL
1.2.7 School Development Plans	No		Life of the plan + 3 years	SECURE DISPOSAL

1.3 Admissions Process				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.3.1 All records relating to the creation and implementation of the School Admissions' Policy	No	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December '14	Life of the policy + 3 years then review	SECURE DISPOSAL
1.3.2 Admissions – if the admission is successful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December '14	Date of admission + 1 year	SECURE DISPOSAL
1.3.3 Admissions – if the appeal is unsuccessful	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014	Resolution of case + 1 year	SECURE DISPOSAL
1.3.4 Register of Admissions	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October '14	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made.(3)	REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
1.3.5 Admissions – Secondary Schools – Casual	Yes		Current year + 1 year	SECURE DISPOSAL

1.3.6 Proofs of address supplied by parents as part of the admissions process	Yes	School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December '14	Current year + 1 year	SECURE DISPOSAL
1.3.7 Supplementary Information form including additional information such as religion, medical conditions etc	Yes			
For successful admissions			This information should be added to the pupil file	SECURE DISPOSAL
For unsuccessful admissions			Until appeals process completed	SECURE DISPOSAL
1.4 Operational Administration				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
1.4.1 General file series	No		Current year + 5 years then REVIEW	SECURE DISPOSAL
1.4.2 Records relating to the creation and publication of the school brochure or prospectus	No		Current year + 3 years	STANDARD DISPOSAL
1.4.3 Records relating to the creation and distribution of circulars to staff, parents or pupils	No		Current year + 1 year	STANDARD DISPOSAL
1.4.4 Newsletters and other items with a short operational use	No		Current year + 1 year	STANDARD DISPOSAL
1.4.5 Visitors' Books and Signing in Sheets	Yes		Current year + 6 years then REVIEW	SECURE DISPOSAL
1.4.6 Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations	No		Current year + 6 years then REVIEW	SECURE DISPOSAL
2. Human Resources - This section deals with all matters of Human Resources management within the school.				
2.1 Recruitment				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.1.1 All records leading up to the appointment of a new headteacher	Yes		Date of appointment + 6 years	SECURE DISPOSAL
2.1.2 All records leading up to the appointment of a new member of staff – unsuccessful candidates	Yes		Date of appointment of successful candidate + 6 months	SECURE DISPOSAL

2.13 All records leading up to the appointment of a new member of staff – successful candidate	Yes		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months	SECURE DISPOSAL
2.1.4 Pre-employment vetting information – DBS Checks	No	DBS Update Service Employer Guide June '14: Keeping children safe in education. July '15 (Statutory Guidance from Dept. of Education) Sections 73, 74	The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months	
2.1.5 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 member of staff's personal file	
2.1.6 Pre-employment vetting information – Evidence proving the right to work in the United Kingdom (4)	Yes	An employer's guide to right to work checks [Home Office May 2015]	Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years	
2.2 Operational Staff Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.2.1 Staff Personal File	Yes	Limitation Act 1980 (Section 2)	Termination of Employment + 6 years	SECURE DISPOSAL
2.2.2 Timesheets	Yes		Current year + 6 years	SECURE DISPOSAL
2.2.3 Annual appraisal/ assessment records	Yes		Current year + 5 years	SECURE DISPOSAL

2.3 Management of Disciplinary and Grievance Processes				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.3.1 Allegation of a child protection nature against a member of staff including where the allegation is unfounded(5)	Yes	"Keeping children safe in education Statutory guidance Sept '18"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March '15"	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2 Disciplinary Proceedings	Yes			
oral warning			Date of warning(6) + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
written warning – level 1			Date of warning + 6 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
written warning – level 2			Date of warning + 12 months	SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
final warning Date of warning + 18 months				SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
case not found			If the incident is child protection related then see above otherwise dispose of at the conclusion of the case	SECURE DISPOSAL
2.4 Health and Safety				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.4.1 Health and Safety Policy Statements	No		Life of policy + 3 years	SECURE DISPOSAL
2.4.2 Health and Safety Risk Assessments	No		Life of risk assessment + 3 years	SECURE DISPOSAL
2.4.3 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
2.4.4 Accident Reporting Yes Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980				
Adults			Date of the incident + 6 years	SECURE DISPOSAL
Children			DOB of the child + 25 years	SECURE DISPOSAL

2.4.5 Control of Substances Hazardous to Health (COSHH)	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year + 40 years	SECURE DISPOSAL
2.4.6 Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	SECURE DISPOSAL
2.4.7 Process of monitoring of areas where employees and persons are likely to have become in contact with radiation	No		Last action + 50 years	SECURE DISPOSAL
2.4.8 Fire Precautions log books	No		Current year + 6 years	SECURE DISPOSAL
2.5 Payroll and Pensions				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
2.5.1 Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567)	Current year + 3 years	SECURE DISPOSAL
2.5.2 Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
3. Financial Management of the School - This section deals with all aspects of the financial management of the school including the administration of school meals.				
3.1 Risk Management and Insurance				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.1.1 Employer's Liability Insurance Certificate	No		Closure of the school + 40 years	SECURE DISPOSAL
3.2 Asset Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.2.1 Inventories of furniture and equipment	No		Current year + 6 years	SECURE DISPOSAL
3.2.2 Burglary, theft and vandalism report forms	No		Current year + 6 years	SECURE DISPOSAL
3.3 Accounts and Statements including Budget Management				

Basic File Description	Data Prot Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
3.3.1 Annual Accounts	No		Current year + 6 years	STANDARD DISPOSAL
3.3.2 Loans and grants managed by the school	No		Date of last payment on the loan + 12 years then REVIEW	SECURE DISPOSAL
3.3.3 Student Grant applications	Yes		Current year + 3 years	SECURE DISPOSAL
3.3.4 All records relating to the creation and management of budgets including the Annual Budget statement and background papers	No		Life of the budget + 3 years	SECURE DISPOSAL
3.3.5 Invoices, receipts, order books and requisitions, delivery notices	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.6 Records relating to the collection and banking of monies	No		Current financial year + 6 years	SECURE DISPOSAL
3.3.7 Records relating to the identification and collection of debt	No		Current financial year + 6 years	SECURE DISPOSAL
3.4 Contract Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.4.1 All records relating to the management of contracts under seal	No	Limitation Act 1980	Last payment on the contract + 12 years	SECURE DISPOSAL
3.4.2 All records relating to the management of contracts under signature	No	Limitation Act 1980	Last payment on the contract + 6 year	SECURE DISPOSAL
3.4.3 Records relating to the monitoring of contracts	No		Current year + 2 years	SECURE DISPOSAL
3.5 School Fund				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.5.1 School Fund - Cheque books	No		Current year + 6 years	SECURE DISPOSAL
3.5.2 School Fund - Paying in books	No		Current year + 6 years	SECURE DISPOSAL
3.5.3 School Fund – Ledger	No		Current year + 6 years	SECURE DISPOSAL
3.5.4 School Fund – Invoices	No		Current year + 6 years	SECURE DISPOSAL
3.5.5 School Fund – Receipts	No		Current year + 6 years	SECURE DISPOSAL
3.5.6 School Fund - Bank statements	No		Current year + 6 years	SECURE DISPOSAL
3.5.7 School Fund – Journey Books	No		Current year + 6 years	SECURE DISPOSAL
3.6 School Meals Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
3.6.1 Free School Meals Registers	Yes		Current year + 6 years	SECURE DISPOSAL
3.6.2 School Meals Registers	Yes		Current year + 3 years	SECURE DISPOSAL
3.6.3 School Meals Summary Sheets	No		Current year + 3 years	SECURE DISPOSAL

4. Property Management - This section covers the management of buildings and property.				
4.1 Property Management				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
4.1.1 Title deeds of properties belonging to the school	No		PERMANENT - These should follow the property unless the property has been registered with the Land Registry	
4.1.2 Plans of property belong to the school	No		These should be retained whilst the building belongs to the school and should be passed onto any new owners if the building is leased or sold.	
4.1.3 Leases of property leased by or to the school	No		Expiry of lease + 6 years	SECURE DISPOSAL
4.1.4 Records relating to the letting of school premises	No		Current financial year + 6 years	SECURE DISPOSAL
4.2 Maintenance				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
4.2.1 All records relating to the maintenance of the school carried out by contractors	No		Current year + 6 years	SECURE DISPOSAL
4.2.2 All records relating to the maintenance of the school carried out by school employees including maintenance log books	No		Current year + 6 years	SECURE DISPOSAL
5. Pupil Management - This section includes all records which are created during the time a pupil spends at the school. For information about accident reporting see under Health and Safety				
5.1 Pupil's Educational Record				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.1.1 Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No. 1437		
Primary			Retain whilst the child remains at the primary school	The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more
Secondary		Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	SECURE DISPOSAL

5.1.2 Examination Results – Pupil Copies	Yes			
Public			This information should be added to the pupil file	All uncollected certificates should be returned to the examination board.
Internal			This information should be added to the pupil file	
5.1 Pupil's Educational Record - This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.1.3 Child Protection information held on pupil file	Yes	"Keeping children safe in education Statutory guidance Sept '18"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March '15"	If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file.	SECURE DISPOSAL – these records MUST be shredded
5.1.4 Child protection information held in separate files	Yes	"Keeping children safe in education Statutory guidance Sept '18"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March '15"	DOB of the child + 25 years then review This retention period was agreed in consultation with the Safeguarding Children Group on the understanding that the principal copy of this information will be found on the Local Authority Social Services record	SECURE DISPOSAL – these records MUST be shredded
Note - Retention periods relating to allegations made against adults can be found in the Human Resources section of this retention schedule.				
5.2 Attendance				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.2.1 Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	Every entry in the attendance register must be preserved for a period of three years after the date on which the entry was made.	SECURE DISPOSAL
5.2.2 Correspondence relating to authorized absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
5.3.1 Special Educational Needs files, reviews and Individual Education Plans	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the pupil + 25 years	REVIEW NOTE: This retention period is the minimum retention 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 minimum retention period and this should be documented.
5.3.2 Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement	Yes	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.3 Advice and information provided to parents regarding educational needs	Yes	Special Educational Needs and Disability Act 2001 Section 2	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4 Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Date of birth of the pupil + 25 years [This would normally be retained on the pupil file]	SECURE DISPOSAL unless the document is subject to a legal hold
6. Curriculum Management				
6.1 Statistics and Management Information				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
6.1.1 Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
6.1.2 Examination Results (Schools Copy)	Yes		Current year + 6 years	SECURE DISPOSAL
SATS records	Yes			
Results			The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison	SECURE DISPOSAL
Examination Papers			The examination papers should be kept until any appeals/validation process is complete	SECURE DISPOSAL

6.1.3 Published Admission Number (PAN) Reports	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.4 Value Added and Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
6.1.5 Self Evaluation Forms	Yes		Current year + 6 years	SECURE DISPOSAL
6.2 Implementation of Curriculum				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
6.2.1 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 further retention period or SECURE DISPOSAL
6.2.2 Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.3 Class Record Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.4 Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.5 Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a further retention period or SECURE DISPOSAL
6.2.6 Pupils' Work	No		Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year	SECURE DISPOSAL
7. Extra Curricular Activities				
7.1 Educational Visits outside the Classroom				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
7.1.1 Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Primary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 14 years	SECURE DISPOSAL

7.1.2 Records created by schools to obtain approval to run an Educational Visit outside the Classroom – Secondary Schools	No	Outdoor Education Advisers' Panel National Guidance website http://oeapng.info specifically Section 3 - "Legal Framework and Employer Systems" and Section 4 - "Good Practice".	Date of visit + 10 years	SECURE DISPOSAL
7.1.3 Parental consent forms for school trips where there has been no major incident	Yes		Conclusion of the trip	Although the consent forms could be retained for DOB + 22 years, the requirement for them being needed is low and most schools do not have the storage capacity to retain every single consent form
7.1.4 Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)		DOB of the pupil involved in the incident + 25 years The permission slips for all the pupils on the trip need to be retained to show that
7.2 Walking Bus				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
7.2.1 Walking Bus Registers	Yes		Date of register + 3 years - This takes into account the fact that if there is an incident requiring an accident report the register will be submitted with the accident report and kept for the period of time required for accident reporting	SECURE DISPOSAL [If these records are retained electronically any back up copies should be destroyed at the same time]
7.3 Family Liaison Officers and Home School Liaison Assistants				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
7.3.1 Day Books	Yes		Current year + 2 years then review	
7.3.2 Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst child is attending school and then destroy	
7.3.3 Referral forms	Yes		While the referral is current	
7.3.4 Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	
7.3.5 Contact database entries	Yes		Current year then review, if contact is no longer active then destroy	
7.3.6 Group Registers	Yes		Current year + 2 years	

8. Central Government and Local Authority - This section covers records created in the course of interaction between the school and the local authority.				
8.1 Local Authority				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
8.1.1 Secondary Transfer Sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
8.1.2 Attendance Returns	Yes		Current year + 1 year	SECURE DISPOSAL
8.1.3 School Census Returns	No		Current year + 5 years	SECURE DISPOSAL
8.1.4 Circulars and other information sent from the Local Authority	No		Operational use	SECURE DISPOSAL
8.2 Central Government				
Basic File Description	**Data Prot Issues**	**Statutory Provisions**	**Retention Period (Operational)**	**Action at the end of the administrative life of the record**
8.2.1 OFSTED reports and papers	No		Life of the report then REVIEW	SECURE DISPOSAL
8.2.2 Returns made to central government	No		Current year + 6 years	SECURE DISPOSAL
8.2.3 Circulars and other information sent from central government	No		Operational use	SECURE DISPOSAL

Footnotes:

1 In this context SECURE DISPOSAL should be taken to mean disposal using confidential waste bins, or if the school has the facility, shredding using a cross cut shredder.

2 These are the copies which the clerk to the Governor may wish to retain so that requestors can view all the appropriate information without the clerk needing to print off and collate redacted copies of the minutes each time a request is made.

3 School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014 p6

4 Employers are required to take a "clear copy" of the documents which they are shown as part of this process

5 This review took place as the Independent Inquiry on Child Sexual Abuse was beginning. In light of this, it is recommended that all records relating to child abuse are retained until the Inquiry is completed. This section will then be reviewed again to take into account any recommendations the Inquiry might make concerning record retention

6 Where the warning relates to child protection issues see above. If the disciplinary proceedings relate to a child protection matter please contact your Safeguarding Children Officer for further advice