GDPR Policy

Approved by TCES Operational Board on behalf of

Thomas Keaney, CEO and Schools' Proprietor

Date of next formal review, September 2024

This policy applies to TCES National Online School

Contents

Guidance for the Reader

Notification

In accordance with UK implementation of data protection legislation (the General Data Protection Regulations (GDPR) and any UK enactment thereof) or regulatory requirements, The National Online School have notified the Information Commissioners Office (ICO) for the purpose that we are processing personal data and are on the public register of data controllers.

Policy Review

This policy is reviewed on a yearly basis by the Senior Management Team and the company Management Development Group (School Head Teacher and SLT members) and is signed off accordingly by Schools Proprietor (recorded and indicated as per the front page of this policy).

Policy Conjunction

It is important to note that The National Online School Data Protection policy is written in and should be read in conjunction with the Safeguarding, Child Protection and E-safety/Acceptable Use Policies and that the safety and protection of children and young people educated and cared for by The National Online School are at all times of paramount importance.

This policy is written in line with the GDPR and with reference to; ICO, privacy notice code of practice, security of personal information, information security (principle 7), data protection obligations, individuals rights of access to examination records, the use of biometric technologies in schools, disclosure of exam results to the media, data sharing code of practice, personal information online code of practice, CCTV code of practice 2008, taking photos in schools and outsourcing guide.

Policy Availability

The Data Protection policy is available to all parents/carers in hard copy on request and also available on The National Online School web site.

Please find below details of the School's Data Protection Officer:
Data Protection Officer: Judicium
Address: Judicium Consulting Ltd, 72 Cannon Street, London EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174
Data Protection Lead/Head of Data Services: Craig Stillwell
There is also a parental right to access educational records under 'Education (pupil records) Regulations (NI) 1998' Schools have 15 days to respond.

1 Registration

We are registered as a data controller on the Data Protection Register held by the Information Commissioner – registration number ZB344547. The register can be searched here: https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers

2 Introduction

We collect personal data about the people we deal with during the course of carrying out our business and delivering our services in our schools.

This policy document sets out the approach we take towards managing this personal data to ensure we meet the data protection requirements set out in the General Data Protection Regulation ("GDPR"), any UK specific implementation of aspects of the Regulation into UK law and any guidance the Information Commissioner's Office.

We take data protection seriously and place a high importance on the correct and lawful processing of all personal data as well as respecting the rights and privacy of our clients and employees. As such, this policy sets out the company procedures that are to be followed, by all employees when dealing with personal data across the business.

2.1 Data protection definitions

- The GDPR defines "Personal Data" as data relating to a living individual who can be identified from those data or from other information held by, or likely to come into the possession of, the data controller. The school holds a range of personal data (including personal information about pupils, parents, professional records of staff members and academic information) in digital form and as paper records.
- "Special categories of personal data" relates to more sensitive personal data including racial or ethnic origin, religious beliefs, and health related information. The school will be holding various pieces of special category data such as health records relating to our pupils.
- "Processing" means any activity carried out on the personal data including storage, collection, organisation, and general use.
- A "Data Subject" is the person whose data it is that is being collected or processed by the Data Controller and/or the Data Processor. In school a data subject would include pupils, parents, teachers, etc.
- A "Data Controller" is an organisation, such as our school, who determines the purposes of processing of data – typically this is the organisation that has collected the data in the first place and wishes to process it.
- A "Data Processor" is a person or organisation who processes data on behalf of the Data Controller (usually a third party). This will include any third-party systems we use to process our data.

2.2 Data Protection Principles

Under the GDPR, data controllers must adhere to a range of rules or principles. Personal data should be:

1) Processed fairly, transparently, and lawfully.
2) Obtained only for one or more specified and lawful purposes.
3) Adequate, relevant, and not excessive.
4) Accurate and kept up to date where necessary.
5) Kept for no longer than is necessary for that purpose or those purposes.
6) Protected by appropriate levels of security.

It is up to the Data Controller or Processor to be able to demonstrate compliance with these principles (this is the principle of "accountability")

2.3 Lawfulness of processing

For processing to be lawful, data can only be processed when one of the following conditions apply:

- The Data Subject has given consent.
- Processing is required for the performance of a contract or delivering a service.
- Processing is required to comply with a legal obligation.
- Processing is necessary to protect the vital interests of the Data Subject
- Processing is carried out in the public interest.
- Processing is carried out in the legitimate interests of the Data Controller, but without detriment to the Data Subject.

2.4. Data subject rights

Under the GDPR, Data Subjects have the following rights:

- The right to be informed (including when the data was not obtained directly from them) about who has their data, what it's used for, who will have access to and their rights to object, withdraw consent, etc.
- The right to request whether data is being processed by the Data Controller and if so what data and how to request a copy of the data (this is a subject access request)
- The right to have their data updated and kept up to date.
- The right to erasure of their data when the data is no longer needed, when consent has been withdrawn or if it has been unlawfully processed.
- To restrict, in certain circumstances, the processing of their data.
- The right to data portability allowing a Data Subject to request copies of their data in a format compatible with another system for their own use or to import into a third-party system.
- The right to object to the processing under legitimate interests, for direct marketing purposes, for profiling or research.

- The right to object to automated decision making.

2.5 General Statement

We are fully committed to upholding the above principles and will:

- Inform individuals why personal information is collected.
- Notify individuals when their data is shared and explain why and with whom it was shared.
- Maintain the quality and accuracy of personal data.
- Not retain information for longer than necessary.
- Destroy any information that is no longer needed appropriately and securely.
- Protect all personal information from loss, theft, and unauthorised disclosure.
- Share information with others only when legally appropriate.
- Set out procedures to ensure compliance with Subject Access Requests and other individual rights.
- Make sure all staff are fully aware of our policies.

3 Roles and responsibilities

All employees have a responsibility to ensure data protection compliance, however, these people have key areas of responsibility:

Board of Directors
The Board is ultimately responsible for ensuring adequate data protection controls are in place across the business.

Data Protection Officer
The Data Protection Officer is responsible for:

- Overall data protection compliance for the business.
- Reviewing (annually) all data protection resources made available to the business, including this policy, guidance, and support information.

The Data Protection Manager is responsible for:

- Keeping the Board updated about data protection responsibilities, risks, and issues across the business.
- Ensuring adequate training is in place for all employees, plus specific training for the [marketing / sales / support / customer services] teams.
- Dealing with data protection and privacy related questions from any part of the business.
- Dealing with subject access requests from Data Subjects (pupils, parents, or employees).

- Dealing with any requests to access data (pupils, parents or employees) from external third parties, for example law enforcement and government offices.
- Carrying out due diligence and ensuring appropriate contractual terms are in place for any third parties we use to share or store personal data.
- We use an external agency to act as our Data Protection Officer although we have an internal Data Protection Manager:

Data Protection Manager:
Address: TCES, 3rd Floor, Beacon House, 26-28 Worple Road, Wimbledon, SW19 4EE Telephone 020 8545 4950

Data Protection Officer: Judicium
Address: Judicium Consulting Ltd, 72 Cannon Street, London EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9172
Data Protection Lead/Head of Data: Craig Stillwell.

IT Manager

The IT Manager is responsible for:

- Ensuring all IT systems and use of technology is compliant and in line with this policy.
- Maintaining IT security across the business and ensuring the security of systems is kept up to date.
- Assisting the Data Protection Officer with assessing the security aspects of any third-party systems that may be used to handle the company's data.

Marketing Manager

- The Marketing Manager is responsible for ensuring all marketing is compliant with the GDPR rules relating to consent and the marketing rules as set out in the Privacy and Electronic Communications Regulations ("PECR").

HR Manager

- HR are responsible for ensuring that employee data is processed in line with this policy and any other rules or guidance relating to the use of employee data.

All employees

- All employees will familiarise themselves with this policy and any associated policies, relating to the processing of personal data and ensure their processing of personal data is within the rules set out within these policy documents. Specifically, all employees should ensure:

- All personal data accessed, used, or processed during their duties is kept and processed securely.
- No personal data should be disclosed verbally, in writing or by any other means to any third party, without consent from the company's Data Protection Officer
- No company systems should be accessed for any reason other than for the purposes of carrying out their duties as an employee.
- They contact the Data Protection Officer if they are aware of an issue or are uncertain about any aspect of processing data.

4 Fair Processing

The National Online School, as required by the GDPR, issue a Privacy Notice to parents/carers to inform them and their children of the purposes for which their personal data may be held. In the case of pupils over 13 the notice is issued to the pupil. (Please see appendix 1 – Privacy Notice) – This Privacy Notice can also be found on our website. *Please see section 9 of this policy regarding CCTV.*

5 Collection of personal data

5.1 Whenever we collect data, we will only ask for data that is needed. What we collect will depend on the circumstances for which the data is to be used and this will be obvious to the individual whose data it is

5.2 Where we need consent for the purposes of processing we will:

- Be open and transparent about why we are collecting the data and what is being consented to
- Provide an option for the Data Subject to provide their consent.
- We will not provide any pre-ticked options or use any wording that could be missed or misconstrued by the Data Subject to "trick" them into consenting.
- We will record the place, time, and situation by which that consent was given.

5.3 In all circumstances, when collecting data, we will provide the following information:

- Details of who we are, why we're collecting the data, what it will be used for and how long we will use and keep the data, and the legal basis for processing.
- Details of our Data Protection Officer and how they can be contacted.
- Details of the Data Subject's rights:
  - Data Subject access requests.
  - Have their data corrected if details change.
  - Have their data deleted when it is no longer needed.
  - Object to processing.
  - Right to complain to the Information Commissioner's Office.

- Details of how to withdraw consent (when consent is the lawful basis of processing).

5.4. Where we make use of data supplied by a third party, in addition to the items listed in 5.3, we will also provide details of where the data came from. The information will be given to the Data Subject at the first opportunity (but not more than one calendar month from receiving the data).

6 Use of personal data

6.1. We will only process personal data supplied to us for its original purpose. We will not reuse the data for any other purpose unless it is lawful for us to do so (e.g., we have consent from the Data Subject).

6.2. Where "legitimate interest" is the lawful basis for processing it will be possible to demonstrate that such processing is not harmful to the Data Subject's rights and the reason for processing as a legitimate interest, will be documented.

6.3. Where personal data is held by us for marketing purposes, it is the responsibility of the Marketing Manager to ensure that before, each time, data is used, it is cleansed against relevant marketing preference databases (e.g. Telephone Preference Services, Mail Preference Service and Corporate Mail Preference Service) to ensure that the Data Subjects have not opted out of marketing, or withdrawn consent and that any electronic marketing meets the requirements of the Privacy and Electronic Communications Regulations 2003.

7 Information Security

7.1 Physical Security and procedures

Our ICT systems include security measures to prevent unauthorised users from accessing protected files. All staff are assigned a role and clearance which will determine their access to protected data.

Staff must set strong passwords, change them regularly, and never share them. Personal data will only be accessed from password protected devices which should be locked when not in use. We will take appropriate steps to keep data storage media physically secure. Policy password processes must be followed.

Data is backed up daily. *Please see section 9 of this policy in relation to CCTV*

7.2 Portable electronic devices

All portable electronic devices are kept as securely as possible on and off from school premises.

Removable media (portable hard drives) should only be used, to store personal data, with permission from a senior member of staff and only **if** it is password

protected and has approved virus and malware checking software. The data should be encrypted and securely deleted when it is no longer in use.

Under no circumstances should USBs be used in the company to save data or transfer data. (Unless this is CCTV footage for a specific reason). No external USBs should be bought into the company and plugged into a company PC or laptop.

7.3 Electronic personal data.

When transferring personal data to the local authority or other agencies, or for members of staff to access personal information outside of school.

- Staff must have permission to access or transfer the data out of school and use appropriately secured encrypted system.
- Devices containing personal data may only be accessed by authorised staff.
- Where possible, personal data should be accessed via secure remote access to the school's management information system.
- Staff must securely store and protect any personal devices used to access data.
- Documents should be password protected and names should not be used in the subject title.
- Sensitive data must not be stored in remote or cloud storage or on desktop PCs.

The local authority should be consulted if it is necessary to transfer data to another country.

7.4 Use of private computer equipment - BYOD or 'bring your own device'. This must be agreed by the National Online School.

The school is responsible for school data that you process on personal devices. If you use your own device for schoolwork you will need to ensure that you meet the National Online School responsibilities for data handling, which includes allowing access to your personal device if necessary. You must have the agreement of your manager to use your own device in school and we may have to refuse some access requests for security reasons.

Security - When you use a personal device for schoolwork you must ensure you keep personal data secure. Where appropriate and depending on the device, you will need to install the school approved software before using a personal device for schoolwork. You should always ensure that you have set secure passwords on all your devices including mobile phones. Before using your own device in school, you need to know how to:

- prevent loss, theft, or unauthorised access of data.
- keep sensitive information confidential.
- maintain the security and integrity of information.

You must delete sensitive documents including emails when you have finished working on them and make sure that you limit the amount of data that syncs to your device.

Loss and theft **-** If your personal device has been used for school business and is lost or stolen, you must change your password for all school services accessed from your device and report the incident to the Head Teacher who will inform the National Online School e-safety officer and Data Protection Officer as soon as possible.

The e-safety officer and Data Protection Officer will liaise with Wanstor (ICT) who will take steps to ensure the security of school data which may include a remote wipe of data (removing all school data from your device). This may result in the loss of any personal information stored on the device.

Some school data is highly sensitive and should never be 'stored' on a personal device. If you are unsure about what information can be stored or the protections you should use, you should ask for guidance from your line manager.

Use and conduct – When using your personal device for schoolwork you must abide by the National Online School ICT and e-safety/acceptable use / ICT policy.

7.5 Paper based personal data:

Child personal data:

- Child protection data is kept in a stand-alone locked safe bolted to a secure surface and accessible by Head Teacher and Business Manager only.
- Exam documentation is kept in a locked exams safe in a room with no windows and is accessible by the Exams Officer only.
- Pupil files are kept in a locked cabinet and accessible by Head Teacher and Senior Leadership Team only.
- Referrals paperwork is kept in a locked cabinet and accessed by Business Development department personnel only.

Staff personal data:

- All staff personal information is kept in the HR department in a locked cabinet and accessible by HR personnel only.
- Finance information is kept in a locked cabinet and accessible by finance personnel only.
- Allegations in relation to members of staff is kept in a locked cabinet accessible by the Group Training and Quality Assurance Safeguarding Manager only.
- Information relating to CEO & Schools Proprietor and Board is kept in a locked cabinet by PA to CEO and accessible by CEO or PA only.

7.6 Acceptable Use and Expected Conduct

All Users in the National Online School are responsible for using the ICT systems in accordance with the relevant e-safety/Acceptable Use / ICT Policy and will be asked to sign an Acceptable Use Agreement before being given access to use any ICT systems. All users understand the importance placed on them in relation to misuse or access to inappropriate materials and are aware of the consequences. Likewise, all users acknowledge the importance of reporting abuse, misuse or access to inappropriate materials and know how to do this.

All Users know the importance of adopting good e-safety practices when using digital technologies and that the e-Safety /Acceptable Use / ICT policy covers their actions within and outside of the TCES Group. This includes the use of mobile phones, digital cameras, handheld devices, 'taking and using' images and on cyber-bullying incidents.

All School Staff are responsible for reading the National Online School e-safety/acceptable use/ICT policy and use school ICT systems, accordingly, including the use of mobile phones, and hand-held devices.

All Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

All Parents/Carers will provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to school and know and understand what the 'rules of 'appropriate use' are and what sanctions result from misuse.

8 Records Management

The National Online School recognises that by effectively 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 school. Records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.

The school has responsibility to maintain its records and record keeping systems in accordance with the National Online School process and procedures. The person with overall responsibility for record systems is the Head Teacher who is responsible for records management in the school and will give guidance about good records management practice and will promote compliance so that information will be retrieved easily, appropriately, records stored securely and accessed appropriately and in a timely way.

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

management guidelines. (Please see appendix 1 – Retention Schedule)

9 Accuracy of data and keeping it up to date

- If we are told by a pupil, parent or employee that the data we hold on to them is out of date or incorrect we shall make sure the incorrect data is either deleted or updated.
- If we are updating information about a pupil, we must do so immediately to ensure the old data is not processed in the meantime.
- If we have shared the data with any third party, we will immediately inform the third party to ensure their copies of the data are updated.

10 Sharing Personal Information – Privacy Notice

It may sometimes be necessary to transfer or share personal data with the local authority or other agencies, or for members of staff to access personal information outside of school. In these cases:

- Users must have permission to access or transfer the data out of school and use appropriately secured encrypted systems.
- Devices containing personal data may only be accessed by authorised users.
- Where possible, personal data should be accessed via secure remote access to the school's management information system.
- Users should securely store and protect any personal devices used to access data.

The local authority should be consulted if it is necessary to transfer data to another country.

11. Data Retention

The National Online School has a responsibility to maintain its records and record keeping systems. When doing this, the school will take account of the following factors: -

- The most efficient and effective way of storing records and information.
- The confidential nature of the records and information stored.
- The security of the record systems used.
- Privacy and disclosure; and
- Their accessibility.

11.1 Data Protection

This policy sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the National Online School. The National Online School Data Protection Policy outlines its duties and obligations under the GDPR.

11.2 Retention Schedule

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the school will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by Departmental Manager.

Electronic records will be regularly monitored by Departmental Manager.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements.

11.3 Destruction of Records

Where records have been identified for destruction are disposed of in an appropriate way. All information is reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints, or grievances.

All paper records containing personal information, or sensitive policy information are shredded before disposal wherever possible or disposed of by an appropriate wastepaper merchant with confirmation that shredding has taken place and held by the Finance Department. All electronic information will be deleted.

The Company maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least:

- File reference (or other unique identifier).
- File title/description.
- Number of files; and
- Name of the authorising officer.

11.4 Archiving

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the Data Protection Manager. The appropriate staff member, when archiving documents should record in this list the following information:

- File reference (or other unique identifier).
- File title/description.
- Number of files; and
- Name of the authorising officer.

11.5 Transferring Information to other Media

Where lengthy retention periods have been allocated to records, the National Online School convert paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

11.6 Responsibility and Monitoring

The Data Protection Manager has primary and day-to-day responsibility for implementing this, Policy. The Data Protection Officer, in conjunction with the National Online School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The data protection officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining, and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

12 Subject Access Request

The right of access by a Data Subject is one of several individuals' rights available to a Data Subject. Article 15 of the GDPR states that a Data Subject has the right to ask a Data Controller about whether they process data about them and if so, to receive information about how their data is processed and to receive a copy of the data. Specifically, the Data Controller must supply information about:

- The purposes of processing.
- The types of data being processed.
- Who has access to the data, including any third parties the data has been shared with.
- How long the data will be processed for.
- The rights the Data Subject has regarding the rectification, erasure, and restrictions on processing of their data.
- The right to lodge a complaint with the Information Commissioner's Office
- The source of the data if it was not directly collected from the Data Subject
- Details of any automated decision making (e.g., profiling) carried out using the data.
- Details of any decisions made about sharing the data with third parties outside the EU.

Subject access requests must be responded to within one month and without due delay.

12.1. Process for dealing with a subject access request

- Subject access requests will be dealt with as a matter of priority and by law must be dealt with, within one month of receiving the request.
- If it is unlikely that the request can be satisfied within the one-month timescale, this must be communicated to the Data Subject along with details of why a delay will occur, within one month of the receiving the request. There needs to be good justification for a delay which should be recorded.
- If it is decided that the request will not be processed, this must be communicated to the Data Subject within one month of the request, explaining why we will not be honouring the request. We must also provide details of how the Data Subject can register a complaint to the Information Commissioner's Office. Any decision not to supply any information to the Data Subject should be recorded.
- The identity of the person making the subject access request should be verified to ensure they are indeed the Data Subject that the information request relates to. How identity is verified will depend on how the request is made, but this must be achieved as soon as possible, so as not to delay the ability to process the request within the one-month deadline.

Appropriate ways to verify identity of the requester:

- By calling the Data Subject using a phone number stored within the data we process; if the Data Subject calls to make the request, even if a CLI is present, you must make it clear that you need to verify identity and use an alternative means to verify identity before disclosing any information – do not trust the CLI to be genuine.
- By emailing the Data Subject using an email address held on file. If the request is made via email, you must find an alternative way to verify identity, even if the request appears to have come from the same email address as the one you have on file.
- Asking the caller or emailer to verify a certain piece of data which would only be known by the Data Subject, such as how an account is paid for, the last 4 digits of the credit card on file, a pre-agreed passphrase, etc.
- Any verification of identity must be carried out without delay so as not to limit the chance of dealing with the subject access request within the one-month time limit.
- Where a subject access request is being made on behalf of the Data Subject (e.g., a legal professional, a parent on behalf of a pupil), the release of the data should be verified with the Data Subject first. It should also be explained to the Data Subject if there will be any data that the Data Subject might find sensitive. If there is any doubt in being able to confirm the identity of the third party or if it is felt the data may be sensitive, the response to the request should be supplied to the Data Subject rather than the requester.

- Under no circumstances should data be released to a third party (through the subject access request process) without the permission of the Data Subject.
- If it is not clear what data is being requested the Data Protection Officer must ask the requester for more information to be able to satisfy the request. This should be done as soon as possible to ensure the one-month deadline for providing the information can still be met. It should be explained that we will be unable to deal with their request until the additional information is provided.
- All data requested should be collected together by the Data Protection Officer. Where the data comes from multiple sources across the business and where other employees are required to help locate or provide the data, those employees must assist the Data Protection Officer in a way which meets the time requirements (one month) of the request. Where the assister is unable to meet the requirements within a timely manner (to meet the one-month deadline) they should tell the Data Protection Officer as soon as possible to ensure the Data Protection Officer has enough time to notify the requester there will be a delay in supplying the information requested.
- All personal data related to the request will be provided, this will include notes on an account, copies of email, transcripts, or recordings of telephone calls (if available), etc. This also means that data held in archives or backups must also be provided if it's relevant to the request and can be easily accessed.
- No data should be deleted to avoid supplying it as part of a subject access request. If the information is available at the time of the request, it must be made available to the requester. This means that special care should be taken if there is data due for deletion or amendment as part of a routine process that could form part of the subject access request – this is why subject access requests should be treated with urgency.
- Once the data requested has been collected it should be checked, before being sent to the requester, to make sure it does not include any information relating to any other Data Subjects. Any personal data relating to a third-party Data Subject must be redacted or permission sought from that third-party, that the data can be included.
- When the request is sent via electronic means, unless requested otherwise, the information should be provided in electronic means. Where the request is made via other means, the Data Protection Officer will ask the requester how they would like to receive the response to their request.
- When the information is supplied via electronic means it will either be encrypted or locked with a password to prevent unlawful access. Where the material is locked (e.g., a password protected PDF or Word document) the password to unlock the material will meet the company requirements for password strength and supplied separately to the requester (preferably via an alternative communication method).

- Explanations of the data supplied should be provided when it's not obvious what it relates to. All explanations about processing and what data is supplied should be in plain English and not use jargon or abbreviations (unless definitions of the jargon or abbreviations are also provided).
- The Data Protection Officer should maintain a record of requests processed with a summary (i.e., not the actual data) of what was supplied, issues, etc.

12.2. Fees

The information will be provided free of charge except when the request is:

- Manifestly unfounded.
- Excessive.
- Or if it's a repetitive request.
- The Data Protection Officer will determine whether a fee can be charged.
- If a fee is to be charged it must be reasonable and only cover the admin costs for providing the data.

- When a fee is chargeable, this should be stated to the requester as soon as possible, allowing them to reject the fee or change their mind about their request in enough time to still be able to provide the information within the one-month time limit. Information should also be provided setting out why a fee is being charged and the justification for charging.

13. Right to erasure

- All requests from a Data Subject for the deletion of their data should be dealt with in consultation with the Data Protection Officer to ensure we don't delete data we have a lawful basis, or legal requirement, to continue processing.
- Unless where we can demonstrate otherwise, if a Data Subject requests the deletion of their data we will comply with the request, within one month of the request, and confirm to the Data Subject what data has been deleted.
- Where the personal data in question has been disclosed to a third party, we will notify the third party of the need for them to also erase the data.

14. Right to data portability

- The IT team will ensure that any systems we use that meets the requirements for a data portability option has the data portability option available either directly to the customer or for a member of the customer services team to activate.
- Where this system is not accessible directly to the Data Subject, all requests for an export of a data from a Data Subject will be dealt with by the Data Protection Officer within one month of the original request.
- The data will be made available at least in CSV format or in a format standard that has been established between suppliers of similar systems.

15. Objections to processing

- Any objections to the use of data for marketing (e.g., requests to stop receiving marketing information) should be passed to the Marketing Manager. The Marketing Manager will ensure that the details of the Data Subject are removed from any marketing lists.
- Any other objections are to be dealt with by the Data Protection Officer to ensure that the business does not have a lawful basis for processing.

16. Third party due diligence

- Where a third party is used for the processing of personal data, due diligence checks will be carried out on the third party, in consultation with the Data Protection Officer, to ensure they are data protection compliant and will enable our own data protection compliance. Such checks will include asking about how they are GDPR compliant and asking them for a GDPR statement.
- Contractual obligations will also be put in place with any third parties we use. Where we provide a contract to be agreed with the third party, we shall ensure these contractual obligations are included in the contract either via a new contract or by an addendum to an existing contract; where we are taking a service from a third party who have their own terms of service, to which we have to agree, we must ensure that the contractual obligations are included within those terms.
- We will not use any third party who is unable to provide evidence of their data protection compliance or willingness to agree to the appropriate contractual terms.

17. Data protection impact assessments

- When new technologies, systems or processes are introduced the Data Protection Officer should be involved and carry out a Data Protection Impact Assessment to ensure the new technologies are compliant with the data protection rules and protect, by default, the privacy, and rights of the Data Subjects whose data will be processed by the new technology. Consideration by the Data Protection Office should include:
  - The purposes for which personal data is being processed and the kinds of processing carried out.
  - An assessment of the necessity and proportionality of the processing with respect to the purposes for which it is being processes.
  - An assessment of the risks to the Data Subjects from the processing
  - Details of steps to be taken to minimise any risk to the Data Subjects from the processing.

18. Data breaches

- A data breach occurs when any personal data is processed or accessed unlawfully. This may be due to a breach in security but relates to the situation

where data is accessed, destroyed, or altered and lost or disclosed, without the appropriate authority.

- All employees have a duty to report any suspected breaches of data protection to the Data Protection Officer. If an employee is in any doubt as to whether a breach has occurred, they must report it to the Data Protection Office regardless.
- Any data breaches will be handled by the Data Protection Officer.

19. Access by third parties

- Any requests to access employee, pupil, or parent data from external parties such as the Police or a government department, should be checked by the Data Protection Officer to ensure it is lawful for us to disclose the data requested.

20. Complaints

- Any complaints made to us about the processing of personal data are to be passed, immediately, to the Data Protection Officer. This includes complaints from data subjects and information requests or correspondence from the information Commissioner's Office

21. International transfer

- The company may, from time to time, transfer, or process personal data outside the EU. Transfer or processing of data outside the EU will only take place when:
  - The transfer is to a country that the European Commission has determined ensures an adequate level of protection for personal data
  - The transfer is to a country or organisation which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the Information Commissioner's Office; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the ICO
  - The transfer is made with the informed consent of the relevant Data Subjects
  - The transfer is necessary for the performance of a contract between the Data Subject and us (or for pre-contractual steps taken at the request of the Data Subject)
- When data is to be transferred, or processed outside the EU for the first time the transfer must be authorised by the Data Protection Officer

22 Website

The purpose of the National Online School website in relation to parents/carers is to help parents/carers and pupils view information about their school and read privacy notices.

The school will comply with the GDPR and ensure that we have parents/carers permission before taking and using images of pupils on the National Online School website. We will also ensure that when images are published on the website that pupils cannot be identified by name unless permission has been obtained upfront, as per the use of photos policy set out below.

We ensure that:

- Pupils are aware that all material must be the author's own work, or where permission to reproduce has been obtained, clearly marked with the copyright owner's name.
- Home information or individual e-mail identities are not published.
- Photographs will not identify individual pupils. Group shots or pictures taken over the shoulder will be used in preference to individual "passport" style.
- Full names will not be used anywhere on the Website, particularly alongside photographs.
- Written permission from parents/carers will be sought before photographs of pupils are published on the National Online School Website.
- Pupils will not be allowed to access public chat rooms.
- New facilities will be thoroughly tested before pupils are given access.

23 Photographs

Digital and video images play an important part in learning activities. Pupils and members of staff may use digital cameras to record activities in lessons and on school trips. These images may then be used in presentations in subsequent lessons.

Images may also be published in newsletters, on the school website and occasionally in local media. (Please see section above regarding the use of images on our website)

In line with the Information Commissioner's Office (ICO), we may take pictures for inclusion in a 'printed' prospectus or school publication without specific consent from parent/carers although we will indicate their intention.

In accordance with guidance from the ICO, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the GDPR). To respect other's privacy (and in some cases for protection) these images should not be published or made publicly available on social networking sites.

Note: we obtain permission from parent/carers on an annual basis consenting to the

use of photographs.

24 Training

Staff awareness is key and underpinned by eight common sense principles or points of good information practice. Staff will be requested to read and sign the data protection Policy to ensure that they understand all processes and procedures and who to pass requests onto. This policy will also form part of the annual all staff abbreviated policy training and will include:

1. What is data protection?
2. What is my schools' approach to data protection?
3. Why do I need to know about data protection?
4. The main data protection principles – what are they?
5. Formal requests – how do I deal with?
6. Telephone enquiries – how do I handle?
7. Can I or should I release information?
8. Staff know what they should be doing and are doing it.

25 Policies

The National Online School has clear and practical polices which affect good governance, backed up by written procedures and where necessary named responsible people.

Policies are reviewed on a yearly basis by the Senior Management Team and the Management Development Group (School Head Teacher and SLT members) and is signed off accordingly by the Schools Proprietor.

26 Freedom of Information Act 2000 (FOIA)

Freedom of Information will be on a case-by-case basis and we may respond to requests in a contextualised manner.

Enquiry/Information Line: 01625 545 700
E Mail: publications@ic-foi.demon.co.uk
Website: www.informationcommissioner.gov.uk

Appendix 1 – Retention Schedule

1. Child Protection					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of life of the record**
1.1	Child Protection file	Yes	Education Act 2002, s175, related guidance "Safeguarding Children in Education", September 2004	DOB + 31 years [1]	SECURE DISPOSAL
1.2	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 Allegations of Abuse against Teachers and Other Staff" November 2005	Until the person's normal retirement age, or 10 years from the date of the allegation whichever is the longer	SECURE DISPOSAL
1.3	Social Care	Yes		75 years	SECURE DISPOSAL

2. Board/Governors					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of life of the record**
2.1	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 should be shredded]
2.2	Agendas	No		Date of meeting	SECURE DISPOSAL
2.3	Reports	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.4	Annual Parents' meeting papers	No		Date of report + 6 years	Retain in school for 6 years from date of meeting
2.5	Instruments of Government	No		Permanent	Retain in school whilst school is open
2.6	Trusts and Endowments	No		Permanent	Retain in school whilst operationally required
2.7	Action Plans	No		Date of action plan + 3 years	SECURE DISPOSAL
2.8	Policy documents	No		Expiry of policy	Retain in school whilst policy is operational (inc if the expired policy is part of a past decision making process)
2.9	Complaints file	Yes		Date of resolution of complaint + 6 years	Retain in school for the six years Review for further retention in the case of contentious disputes. SECURE DISPOSAL routine complaints

2. Board/Governors					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of life of the record**
2.10	Annual Reports required by the Department for Education	No	Education (Governors' Annual Reports) (England) (Amendment) Regulations 2002.SI 2002 No 1171	Date of report + 10 years	
2.11	Proposals for schools to become, or be established as Specialist Status schools	No			Current year + 3 years

3. Management					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
3.1	Log Books	Yes		Date of last entry in the book + 6 years	Retain in the school for 6 years from the date of the last entry
3.2	Minutes of the SMT and other internal administrative bodies	Yes		Date of meeting + 5 years	Retain in the school for 5 years from meeting
3.3	Reports made by the head teacher or the management team	Yes		Date of report + 3 years	Retain in the school for 3 years from meeting
3.4	Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative	Yes		Closure of file + 6 years	SECURE DISPOSAL

3. Management					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
	responsibilities				
3.5	Correspondence created by head teachers, deputy head teachers, and other members of staff with administrative responsibilities	No		Date of correspondence + 3 years	SECURE DISPOSAL
3.6	Professional development plans	Yes		Closure + 6 years	SECURE DISPOSAL
3.7	School development plans	Yes		Closure + 6 years	Review
3.8	Admissions - if the admission is successful	Yes		Admission + 1 year	SECURE DISPOSAL
3.9	Admissions - if the appeal is unsuccessful	Yes		Resolution of case + 1 year	SECURE DISPOSAL
3.10	Admissions - Secondary Schools - Casual	Yes		Current year + 1 year	SECURE DISPOSAL
3.11	Proofs of address supplied by parents as part of the admissions process	Yes		Current year + 1 year	SECURE DISPOSAL
3.12	Supplementary Information form including additional information such as religion, medical conditions etc.				

4. Pupils					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
4.1	Admission Registers	Yes		Date of last entry in the book (or for + 6 years These records are no longer generated in paper but electronically held using Scholarpack software.	Retain in the school for 6 years from the date of the last entry then consider transfer to the Archives
4.2	Attendance registers	Yes		Date of register + 3 years	SECURE DISPOSAL [If these records are retained electronically any backup copies should be destroyed at the same time]
4.3	Pupil Files Retained in Schools	Yes			
4.3a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.3b	• Secondary		Limitation Act 1980	DOB of the pupil + 31 years [3]	SECURE DISPOSAL
4.4	Pupil files	Yes			
4.4a	• Primary			Retain for the time which the pupil remains at the primary school	Transfer to the secondary school (or other primary school) when the child leaves the school.
4.4b	• Secondary		Limitation Act 1980	DOB of the pupil + 31 years	SECURE DISPOSAL
4.5	Special Educational Needs files , reviews and Individual Education Plans	Yes		DOB of the pupil + 31 years the review NOTE: This retention period is the minimum period that any pupil file should be kept. SEN files to be kept for a longer	SECURE DISPOSAL

4. Pupils					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
				period of time to defend the school against 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.	
4.6	Correspondence Relating to Authorised Absence and Issues	No		Date of absence + 2 years	SECURE DISPOSAL
4.7	Examination results	Yes			
4.7a	• Public	No		Year of examinations + 6 years	SECURE DISPOSAL
4.7b	• Internal examination results	Yes		Current year + 5 years **5**	SECURE DISPOSAL
4.8	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 allocate a further retention period or SECURE DISPOSAL
4.9	Statement maintained under The Education Act 1996 - Section 324	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 31 years	SECURE DISPOSAL unless legal action is pending
4.10	Proposed statement or amended statement	Yes	Special Educational Needs and Disability Act 2001 Section 1	DOB + 31 years	SECURE DISPOSAL unless legal action is pending
4.11	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

4. Pupils					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
4.12	Accessibility Strategy	Yes	Special Educational Needs and Disability Act 2001 Section 14	Closure + 12 years	SECURE DISPOSAL unless legal action is pending
4.13	Parental permission slips for school trips - where there has been no major incident	Yes		Conclusion of the trip	SECURE DISPOSAL
4.14	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
4.15	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Primary Schools	No	3-part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 14 years **6**	N
4.16	Records created by schools to obtain approval to run an Educational Visit outside the Classroom - Secondary Schools	No	3-part supplement to the Health & Safety of Pupils on Educational Visits (HASPEV) (1998).	Date of visit + 10 years	N
4.17	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	SECURE DISPOSAL [If these records are retained electronically any back-up copies should be destroyed at the same time]

4. Pupils					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
				kept for the period of time required for accident reporting	

5 Curriculum					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
5.1	School Development Plan	No		Current year + 6 years	SECURE DISPOSAL
5.2	Curriculum returns	No		Current year + 3 years	SECURE DISPOSAL
5.3	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
5.4	Timetable	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.5	Class record books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.6	Mark Books	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL

5 Curriculum					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
5.7	Record of homework set	No		Current year + 1 year	It may be appropriate to review these records at the end of each year and allocate a new retention period or SECURE DISPOSAL
5.8	Pupils' 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
5.9	Examination results	Yes		Current year + 6 years	SECURE DISPOSAL
5.10	SATS records - Examination Papers and Results	Yes		Current year + 6 years	SECURE DISPOSAL
5.11	PAN reports	Yes		Current year + 6 years	SECURE DISPOSAL
5.12	Value Added & Contextual Data	Yes		Current year + 6 years	SECURE DISPOSAL
5.13	Self-Evaluation forms	Yes		Current year + 6 years	SECURE DISPOSAL

6. Personnel Records held in Schools					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
6.1	Timesheets, sick pay	Yes	Financial Regulations	Current year + 6 years	SECURE DISPOSAL
6.2	Staff Personal files	Yes		Termination + 7 years	SECURE DISPOSAL

6. Personnel Records held in Schools					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
6.3	Interview notes and recruitment records	Yes		Date of interview + 6 months	SECURE DISPOSAL
6.4	Pre-employment vetting information (including CRB checks)	No	CRB guidelines	Date of check + 6 months	SECURE DISPOSAL [by the designated member of staff]
6.5	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 DCP for further advice.		
6.5a	• oral warning			Date of warning + 6 months	SECURE DISPOSAL
6.5b	• written warning - level one			Date of warning + 6 months	SECURE DISPOSAL
6.5c	• written warning - level two			Date of warning + 12 months	SECURE DISPOSAL
6.5d	• final warning			Date of warning + 18 months	SECURE DISPOSAL
6.5e	• case not found			If child protection related, please see 1.2 otherwise SECURE DISPOSAL immediately at the conclusion of the case	SECURE DISPOSAL
6.6	Records relating to accident/injury at work	Yes		Date of incident + 12 years In the case of serious accidents, a further retention period will need to be	SECURE DISPOSAL

6. Personnel Records held in Schools					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
				applied	
6.7	Annual appraisal/assessment records	No		Current year + 5 years	SECURE DISPOSAL
6.8	Salary cards	Yes		Last date of employment + 85 years	SECURE DISPOSAL
6.9	Maternity pay records	Yes	Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960), revised 1999 (SI 1999/567)	Current year +3yrs	SECURE DISPOSAL
6.10	Records held under Retirement Benefit Schemes (Information Powers) Regulations 1995	Yes		Current year + 6 years	SECURE DISPOSAL
6.11	Proofs of identity collected as part of the process of checking "portable "enhanced CRB 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	

7. Health and Safety					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
7.1	Accessibility Plans		Disability Discrimination Act	Current year + 6 years	SECURE DISPOSAL

7. Health and Safety					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
7.2	Accident Reporting		Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980		
7.2a	• Adults	Yes		Date of incident + 7 years	SECURE DISPOSAL
7.2b	• Children	Yes		DOB of child + 31 years [8]	SECURE DISPOSAL
7.3	COSHH			Current year + 10 years [where appropriate an additional retention period may be allocated]	
7.4	Incident reports	Yes		Current year + 20 years	SECURE DISPOSAL
7.5	Policy Statements			Date of expiry + 1 year	SECURE DISPOSAL
7.6	Risk Assessments	Yes		Current year + 3 years	SECURE DISPOSAL
7.7	Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos			Last action + 40 years	SECURE DISPOSAL
7.8	Process of monitoring of areas where employees and persons are likely to have come in contact with radiation			Last action + 50 years	SECURE DISPOSAL

7. Health and Safety					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
7.9	Fire Precautions logbooks			Current year + 6 years	SECURE DISPOSAL

8. Administrative					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
8.1	Employer's Liability certificate			Closure of the school + 40 years	SECURE DISPOSAL
8.2	Inventories of equipment & furniture			Current year + 6 years	SECURE DISPOSAL
8.3	General file series			Current year + 5 years	Review to see whether a further retention period is required
8.4	School brochure or prospectus			Current year + 3 years	
8.5	Circulars (staff parents/pupils)			Current year + 1 year	SECURE DISPOSAL
8.6	Newsletters, ephemera			Current year + 1 year	Review to see whether a further retention period is required
8.7	Visitors book			Current year + 2 years	Review to see whether a further retention period is required
8.8	PTA/Old Pupils Associations			Current year + 6 years	Review to see whether a further retention period is required

9. Finance					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
9.1	Annual Accounts		Financial Regulations	Current year + 6 years	
9.2	Loans and grants		Financial Regulations	Date of last payment on loan + 12 years	Review to see whether a further retention period is required
9.3	Contracts				
9.3a	• under seal			Contract completion date + 12 years	SECURE DISPOSAL
9.3b	• under signature			Contract completion date + 6 years	SECURE DISPOSAL
9.3c	• monitoring records			Current year + 2 years	SECURE DISPOSAL
9.4	Copy orders			Current year + 2 years	SECURE DISPOSAL
9.5	Budget reports, budget monitoring etc.			Current year + 3 years	SECURE DISPOSAL
9.6	Invoice, receipts and other records covered by the Financial Regulations		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
9.7	Annual Budget and background papers			Current year + 6 years	SECURE DISPOSAL
9.8	Order books and requisitions			Current year + 6 years	SECURE DISPOSAL
9.9	Delivery Documentation			Current year + 6 years	SECURE DISPOSAL
9.10	Debtors' Records		Limitation Act 1980	Current year + 6 years	SECURE DISPOSAL
9.11	School Fund - Cheque books			Current year + 3 years	SECURE DISPOSAL

9. Finance					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
9.12	School Fund - Paying in books			Current year + 6 years then review	SECURE DISPOSAL
9.13	School Fund - Ledger			Current year + 6 years then review	SECURE DISPOSAL
9.14	School Fund - Invoices			Current year + 6 years then review	SECURE DISPOSAL
9.15	School Fund - Receipts			Current year + 6 years	SECURE DISPOSAL
9.16	School Fund - Bank statements			Current year + 6 years then review	SECURE DISPOSAL
9.17	School Fund - School Journey books			Current year + 6 years then review	SECURE DISPOSAL
9.18	Student grant applications			Current year + 3 years	SECURE DISPOSAL
9.19	Free school meals registers	Yes		Current year + 6 years	SECURE DISPOSAL
9.20	Petty cash books			Current year + 6 years	SECURE DISPOSAL

10. Property					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
10.1	Title Deeds			Permanent	Permanent, these should follow the property unless the property has been registered at the Land Registry
10.2	Plans			Permanent	Retain in school whilst operational

10. Property					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
10.3	Maintenance and contractors		Financial Regulations	Current year + 6 years	SECURE DISPOSAL
10.4	Leases			Expiry of lease + 6 years	SECURE DISPOSAL
10.5	Lettings			Current year + 3 years	SECURE DISPOSAL
10.6	Burglary, theft and vandalism report forms			Current year + 6 years	SECURE DISPOSAL
10.7	Maintenance log books			Current year + 6 years	SECURE DISPOSAL
10.8	Contractors' Reports			Current year + 6 years	SECURE DISPOSAL

11. Local Authority					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
11.1	Secondary transfer sheets (Primary)	Yes		Current year + 2 years	SECURE DISPOSAL
11.2	Attendance returns	Yes		Current year + 1 year	SECURE DISPOSAL
11.3	Circulars from LEA			Whilst required operationally	Review to see whether a further retention period is required

12. Department for Children, Schools and Families					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
12.1	HMI reports			These do not need to be kept any longer	
12.2	OFSTED reports and papers			Replace former report with any new inspection report	Review to see whether a further retention period is required
12.3	Returns			Current year + 6 years	SECURE DISPOSAL
12.4	Circulars from Department for Children, Schools and Families			Whilst operationally required	Review to see whether a further retention period is required

13. Connexions					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
13.1	Service level agreements			Until superseded	SECURE DISPOSAL
13.2	Work Experience agreement			DOB of child + 18 years	SECURE DISPOSAL

14. Schools Meals					
	Basic file description	**DP Issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
14.1	Dinner Register			Current year + 3 years	SECURE DISPOSAL
14.2	School Meals Summary Sheets			Current year + 3 years	SECURE DISPOSAL

15. Family Liaison Officers and Home School Liaison Assistants					
	Basic file description	**DP issues**	**Statutory Provisions**	**Retention Period [operational]**	**Action at the end of the life of the record**
15.1	Day Books	Yes		Current year + 2 years then review	SECURE DISPOSAL
15.2	Reports for outside agencies - where the report has been included on the case file created by the outside agency	Yes		Whilst the child is attending the school then destroy	SECURE DISPOSAL
15.3	Referral forms	Yes		While the referral is current	SECURE DISPOSAL
15.4	Contact data sheets	Yes		Current year then review, if contact is no longer active then destroy	SECURE DISPOSAL
15.5	Contact database entries	Yes		Current year then review if contact is no longer active then destroy	DELETE
15.6	Group Registers	Yes		Current year + 2 years	SECURE DISPOSAL