THE KING'S SCHOOL

DATA PROTECTION POLICY

1. Introduction

- The King's School collects and uses personal information about staff, students, parents and other individuals who come into contact with the school. This information is processed in order to enable the School to provide education and other associated functions. In addition, there may be a legal requirement for the School to process personal information to ensure that it complies with statutory obligations.

- Schools have a duty, as Data Controllers, to keep detailed records of data processing activities and the records shall contain:-

  - Name and details of the organisation (and where applicable, of other controllers, any representative and data protection officer)
  - Purposes of the processing
  - Description of the categories of individuals and categories of personal data.
  - Categories of recipients of personal data
  - Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
  - Retention schedules
  - Description of technical and organisational security measures

  These records must be made available to the Information Commissioner's Office (ICO) upon request. The School will, on an annual basis, provide its registrable particulars and pay the data protection fee to the ICO.

2. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR and DPA and other related legislation. It will apply to personal information regardless of the way it is collected, used, recorded, stored and destroyed and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines and shall attend regular training to ensure compliance with their responsibilities.

3. Key principles

Personal information or data is defined as any information relating to an identifiable person who can be directly or indirectly identified by reference to an identifier held by the school.

Data Protection Principles – there are six enforceable principles contained in Article 5 of the General Data Protection Regulations. They are key to compliance and the School must endeavour to ensure that they are adhered to at all times. The responsibility for adherence to the principles is the responsibilities of all School staff.

3.1.1 Principle 1 – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

3.1.2 Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.1.3 Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary.

3.1.4 Principle 4 – Personal data shall be accurate and where necessary, kept up to date. Steps must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.

3.1.5 Principle 5 - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

3.1.6 Principle 6 - Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

To ensure compliance with the above principles the School will:

(a) Produce an information asset register that contains details of the records it holds.

(b) Inform individuals why the information is being collected at the point it is collected by way of privacy notices.

(c) Inform individuals when their information is shared, and why and with whom it will be shared.

(d) Check the quality and the accuracy of the information it holds.

(e) Ensure that information is not retained for longer than is necessary.

(f) Ensure that when obsolete information is destroyed and it is done so appropriately and securely.

(g) Create, maintain and publish a Disposal and Retention Schedule setting out retention and disposal dates for common data sets and other information.

(h) Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.

(i) Share information with others only when it is fair and lawful to do so and satisfies the lawful basis for processing that information.

(j) Share personal data with other organisations for the purpose of crime prevention and/or detection, or for the purpose of legal proceedings, provided that the disclosure falls within an exemption to the non-disclosure provisions contained within GDPR.

(k) Disclose personal data where required to do so by law for example, following receipt of a court order.

(l) Set out procedures to ensure compliance with the duty to respond to an individual's rights to:
- Request access to personal information, known as Subject Access Requests.
- Be informed about the way their data is used;
- Have inaccurate personal data rectified;
- Have their personal data erased;
- Restrict the processing of their personal data; and
- Object to the processing of their personal data.

(m) Ensure our staff are appropriately and regularly trained and aware of and understand our policies and procedures.

(n) Create and maintain a data breach notification spreadsheet to record data breaches and also circumstances where a breach was narrowly avoided.

4. Data Protection Officer (DPO)

4.1 The Data Protection Officer – our DPO is **Catherine Barnes** and can be contacted on 01476 563180.

4.2 The DPO cannot hold a position that requires them to determine the purpose and means of processing personal data, for example, the Head Master, Head of Human Resources, or Head of Information Technology.

5. Data Protection Impact Assessments (DPIA)

5.1 The School must carry out a DPIA when processing is likely to result in **high risk** to the rights and freedoms of individuals.

5.2 The GDPR does not define high risk but guidance highlights a number of factors that are likely to trigger the need for a DPIA, which include the use of new technologies, processing on a large scale, systematic monitoring, processing of special categories of personal data.

6. Privacy Notices

6.1 The School publishes a privacy notice on its website which provides information about how and why the school gathers and uses images and shares personal data.

6.2 The privacy notice under the GDPR should include:

- Who you are and how they can contact you;
- The personal data being collected & why it is being collected;
- Where the personal data is collected & who it is being sharing with;
- How long the data will be held;
- Transfers to third countries and safeguards;
- Description of the data subjects individual rights;
- The data subjects right to withdraw consent for the processing of their data; and
- How individuals can complain.

6.3 The privacy notice will be reviewed at regular intervals to ensure it reflects current processing.

6.4 The privacy notice will be amended to reflect any changes to the way the School processes personal data.

6.5 Whilst the School will publish an overarching privacy notice it will also issue a privacy notice to all parents and pupils, before, or as soon as possible after, any personal data relating to them is obtained. This may simply be an explanation why the information is being requested and the purpose for which it will be used.

6.6 The privacy notice will include details of how the School uses CCTV, whether it intends to use biometric data and how consent will be requested to do this and include details of the School's policy regarding photographs and electronic images of pupils.

7 Close Circuit Television (CCTV)

7.5 Images and audio recordings of identifiable individuals captured by Closed Circuit Television amount to personal data relating to that individual and will be subject to the same provisions and safeguards afforded by the General Data Protection Regulations and the Data Protection Act as other types of recorded information.

7.6 The School will use CCTV for the following purposes:

- To protect the school buildings and assets;
- To increase personal safety of staff, pupils and visitors;
- To reduce the fear of crime;
- To support the Police in order to deter and detect and to apprehend and prosecute offenders;
- To help protect members of the public and private property;
- To investigate both pupil and staff behaviour where appropriate.

7.7 The School will ensure that any use of CCTV is necessary and proportionate to achieve the aims stated in 7.6.

7.8 The School will ensure that any use of CCTV is included in its records of data processing activity.

7.9 The School's use of CCTV will comply with the Information Commissioner's Office CCTV Code of Practice https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/ .

7.10 The School will ensure that clear notices are in place identifying when an individual is entering an area that is monitored by CCTV. The notice will identify the School as the responsible data controller and will state the purpose for which the recording is taking place.

7.11 The School will not operate audio recording as part of the CCTV without seeking additional advice.

7.12 The School will not operate CCTV in any areas of the premises where individuals would have a legitimate expectation of personal privacy, such as toilets or changing rooms.

7.13 The School will ensure that CCTV recordings are kept securely and that access to them is restricted to those staff that operate the system or make decisions relating to how the images should be used.

7.14 Retain in line with the retention schedule.

8 Photographs and Electronic Images

8.1 As part of school activities we may take photographs and record images of individuals.

8.2 The school will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, the school will explain how the photograph and/or video will be used to both the parent/carer and student.

8.3 Consent can be refused or withdrawn at any time.

9 Biometic Data

9.1 The School uses biometric data (such as fingerprint technology). A notice will be sent to all students and parents explaining the intended reasons and lawful basis for the use of the data, and provide parents with options for alternative systems if they do not wish their son to provide this information and do not want to give consent.

9.2 The School will obtain the written consent of at least one parent or carer with Parental Responsibility for the student before taking and using any biometric data from them (students under 16).

10 Requests for Access to Personal Data

This section sets out the process that will be followed by the school when responding to requests for access to personal data made by a student or their parent or carer with Parental Responsibility.

10.1 There are two distinct rights of access to information held by the school about students, parents/carer and staff:

(a) Students have a right to make a request under the GDPR to access the personal information held about them.

(b) Students and parents or those with Parental Responsibility have a right to access their educational records. The right of those entitled to have access to curricular and educational records is as defined within the Education (Pupil Information) (England) Regulations 2005.

10.2 Handling a subject access request for access to personal data:

10.2.1 Article 15 of the GDPR gives individuals the right to access personal data relating to them, processed by a data controller. The right can be exercised by a person with Parental Responsibility on behalf of their child dependent on the age and the understanding of the child. For the purposes of a subject access request the school will apply the full legal definition of 'Parental Responsibility' when determining who can access a child's personal data.

10.2.2 Requests for information must be made in writing; which can include e-mail, and be addressed to the Head Master. If the original request does not clearly identify the information required, then the School will seek further enquiries to clarify what information is being requested.

10.2.3 The identity of the requestor must be established before the disclosure of any information is made. Proof of the relationship with the child (if not known) must also be

established as this will verify whether the individual making the request can lawfully exercise that right on behalf of the child. Below are some examples of documents which can be used to establish identity:

- Passport
- Driving licence
- Utility bill with current address
- Birth/marriage certificate
- P45/P60
- Credit card or mortgage statement.

10.2.4 A student with competency to understand can refuse to consent to a request for their personal information made under the GDPR. This position differs when the request is for access to the Education Record of the child (see below for more detail).

10.2.5 No charge can be made for access to personal data that is not contained within an education record.

10.2.6 The response time for a subject access request is one month from the date of the request (irrespective of school holiday periods). The one month period will not commence until any necessary clarification of information is sought. The time to respond can be extended to two months where the request is complex or numerous.

10.2.7 There are some exemptions available under the Data Protection Act which will mean that occasionally personal data will need to be redacted (information blacked out/removed) or withheld from the disclosure. All information will be reviewed prior to disclosure to ensure that the intended disclosure complies with the School's legal obligations.

10.2.8 Where the personal data also relates to another individual who can be identified from the information, the information will be redacted to remove the information that identifies the third party. If it is not possible to separate the information relating to the third party from the information relating to the subject of the request, consideration will be given to withholding the information from disclosure. These considerations can be complex and additional advice will be sought when necessary.

10.2.9 Any information which may cause serious harm to the physical or mental health or emotional condition of the student or another person will be withheld along with any information that would reveal that the student is at risk of abuse, or information relating to Court Proceedings.

10.2.10 Where redaction has taken place then a full copy of the information provided will be retained in order to maintain a record of what was redacted and why and a clear explanation of any redactions will be provided in the School's response to the request.

10.2.11 If there are concerns about the disclosure of information additional advice will be sought.

10.3 Handling a request for access to a curricular and educational record as defined within the Education (Pupil Information) (England) Regulations 2005.

10.3.1 A parent may make a request to access information contained within their student's education record, regardless of whether the student agrees to the disclosure of information to them. The right of access belongs to the parent in these cases. It is not a right being exercised by the parent on behalf of the student.

10.3.2 For the purpose of responding to an Educational Records request, the School will apply the definition of 'parent' contained within the Education Act 1996.

10.3.3 An "educational record" means any record of information which-

a. Is processed by or on behalf of the governing body of, or a teacher at, any school maintained by a local education authority and any special school which is not so maintained.
b. Relates to any person who is or has been a student at any such school; and
c. Originated from or was supplied by or on behalf of the persons specified in paragraph (a), other than information which is processed by a teacher solely for the teacher's own use

10.3.4 The amount that can be charged for a copy of information contained in an education record will depend upon the number of pages provided. The charge made will be in accordance with the Education (Pupil Information) (England) Regulations 2005.

10.3.5 No charge will be made to view the education record.

10.3.6 The response time for requests made under the Education (Pupil Information) (England) Regulations 2005 is 15 school days (this does not include half terms or teacher training days).

10.3.7 An exemption from the obligation to comply with the request will be claimed where the disclosure of the information to the parent may cause serious harm to the physical or mental or emotional condition of the student or another person or if the disclosure of the information would reveal that the student is at risk of abuse.

10.3.8 If a subject access request is made for information containing in whole or in part a student's educational record a response must be provided within 15 school days

11. Retention and Disposal of personal data

11.1 The Governing Body will ensure that the School has a up to date and accurate retention and disposal schedule that is compliant with the GDPR. The School will ensure that personal data is stored, transferred and disposed of securely and in accordance with the retention and disposal schedule.

12. Security of personal data

12.1 The School will ensure that appropriate security measures are in place and enforced to keep paper and electronic personal data secure.

12.2 The School will regularly review the physical security of the School buildings and storage systems.

12.3 The School will ensure that only authorised individuals have access to personal data.

12.4 All portable electronic devices containing personal data will be encrypted.

12.5 Personal USB storage containing sensitive, identifiable staff or student data must not be used.

12.6 No personal data will be left unattended in any vehicles and staff will ensure that if it is necessary to take personal data from School premises, for example to complete work from home, the data is suitably secured.

12.7 The School will refer to any relevant guidance and seek advice where necessary if processing personal data utilising a cloud based solution.

13. Complaints

13.1 Complaints relating to the School's compliance with the GDPR will be dealt with in accordance with the school's complaint policy.

13.2 Complaints relating to access to personal information or access to education records should be made to The Head Master who will decide whether it is appropriate for the complaint to be dealt with through the School's complaints procedure. Complaints which are not appropriate to

be dealt with through the school's complaints procedure can be referred to the Information Commissioner. Details of how to make a complaint to the ICO will be provided with the response letter. [Reference to the ICO should only usually be made where the Schools internal complainants process has been exhausted]

13.3. Complaints relating to information handling may be referred to the Information Commissioner's Office (the statutory regulator). Contact details can be found on their website at www.ico.org.uk or telephone 01625 5457453

14. Review

14.1 This policy will be reviewed every two years. The policy review will be undertaken by the Head Master.

15. Contacts

15.1 If you have any enquiries in relation to this policy, please contact the Head Master.

15.2 Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk or telephone 01625 5457453

Policy adopted by Governors: **22 May 2018**
Date of last review: **May 2018**
Review date: **May 2020**

APPENDIX 1: PRIVACY NOTICE EMPLOYEES

THE KING'S SCHOOL

Privacy Notice

(How we use school workforce information)

We process personal data relating to those we employ to work at, or otherwise engage to work at, the school. This is for employment purposes to assist in the running of the school or to enable individuals to be paid. The collection of this information will benefit both national and local users.

The Privacy Notice replaces The Fair Processing Notice (FPN) and should not require annual revisions. Schools, Local Authorities (LA), the Department for Education (DfE) and other educational bodies that process personal data about students and staff are required by the Data Protection Act (1998) to issue a Notice to parents, students and staff to inform them of the purposes for which that personal data may be held and used. The new process will mean much simpler Privacy Notices, where details of any organisations with which the LA and DfE share data are contained on the LA and DfE websites, with links from the Privacy Notices. This means that Privacy Notices do not need re-issuing on an annual basis. The aim is to make the Privacy Notices issued to students and staff general and constant. Any changes to the details of organisations with which school or LA data is shared can be updated on the LA and DfE websites.

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

- Personal information (such as name, employee or teacher number, national insurance number)
- Special categories of data including characteristics information such as gender, age, ethnic group
- Contract information (such as start dates, hours worked, post, roles and salary information)
- Work absence information (such as number of absences and reasons)
- Qualifications (and, where relevant, subjects taught)
- Medical information (such as food allergies or medication needed in an emergency)
- Contact information (such as telephone numbers of contacts that an employee would want the school to contact in an emergency)
- Address information (such as the known contact address to direct correspondence to)
- Payroll information (such as bank account numbers for payment transfers)

We also process special categories of personal data that may include:

- Physical or mental health needs
- Racial or ethnic origin
- Trade union membership
- Political affiliation and political opinions
- Criminal convictions data
- Civil and criminal proceedings, outcomes and sentences.
- Religious or other beliefs of a similar nature

Why we collect and use this information

We use school workforce data to:

- Enable the development of a comprehensive picture of the workforce and how it is deployed
- Inform the development of recruitment and retention policies
- Enable individuals to be paid
- To contact employees directly when they are not on the premises
- To contact others known to the employee, where the employee has provided their information, in cases where it would be reasonable for us to contact that individual.

The lawful basis on which we process this information

We collect and use information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as Departmental Censuses under the Education Act 1996 and other such data processes that relate education provision or payment of the individual. Further information is available at https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information
Whilst the majority of information an employee provides is mandatory, some of it is given on a voluntary basis. In order to comply with data protection legislation, the school will inform you whether employees are required to provide certain school workforce information or if they have a choice.

Storing this information
The school holds school workforce data in line with its Data Retention Guidelines - see appendix 3.

This information is shared with:

- The Department for Education (DfE)
- Our payroll provider
- Our HR provider
- Teachers' Pensions
- LGPS
- Please follow the link to access other suppliers who act as Data Controller or Data Processor: Copy of List of companies acting as Data Processor and or Data Controller.xlsx

Sharing workforce information
The School does not share information about employees with anyone without consent unless the law and our policies allow us to do so.

Local authority
The School is required to share information about employees with Lincolnshire local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

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

The School is required to share information about our students with the (DfE) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Data collection requirements
The DfE collects and processes personal data relating to those employed by schools (including Multi Academy Trusts) and local authorities that work in state funded schools. All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005.

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

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

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

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

- Who is requesting the data
- The purpose for which it is required

- The level and sensitivity of data requested; and
- The arrangements in place to securely store and handle the data

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

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

Requesting access to personal data
Under data protection legislation, an employee has the right to request access to information the school holds about them. To make a request, contact Catherine Barnes, Bursar & Director of Resources / Data Protection Officer admin@kings.lincs.sch.uk

An employee also has the right to:
- Object to processing of personal data that is likely to cause, or is causing, damage or distress
- Prevent processing for the purpose of direct marketing
- Object to decisions being taken by automated means
- In certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- Claim compensation for damages caused by a breach of the Data Protection regulations

If an employee has a concern about the way the school is collecting or using their personal data, they should raise their concern with the Head Master in the first instance. Alternatively, an employee can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If an employee would like to discuss anything in this privacy notice, please contact: Catherine Barnes, Bursar & Director of Resources / Data Protection Officer

APPENDIX 2 PRIVACY NOTICE - STUDENTS

THE KING'S SCHOOL

Privacy Notice

(How we use student information)

We collect and hold personal information relating to our students and may also receive information about them from their previous school. The school uses and processes student information within the remit of the Regulation (EU) 2016/679 (General Data Protection Regulation), referred to throughout this statement as the GDPR.

The Privacy Notice replaces The Fair Processing Notice (FPN) and should not require annual revision. Schools, Local Authorities (LA), the Department for Education (DfE) and other educational bodies that process personal data about students and staff are required by the Data Protection Act (1998) to issue a Notice to parents, students and staff to inform them of the purposes for which that personal data may be held and used.

The aim is to make the Privacy Notices issued to students and staff general and constant. Any changes to the details of organisations with which school or LA data is shared can be updated on the LA and DfE websites.

The categories of student information that the school collects, holds and shares include:

- Personal information (such as name, unique student number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and reasons for absence)
- Assessment information (such as internal tests, student progress information and examination results)
- Medical information (such as allergies to food, medication a student may require and medical incidents that have occurred inside or outside of school that may affect learning)
- Special Educational Needs and Disabilities information (such as specific learning difficulties, specific medical needs and previous learning or medical needs)
- Behaviour information (such as rewards, achievements, incident records and exclusions)
- Post 16 information (such as destinations data, UCAS applications and grants)

The school also processes special categories of personal data that may include:

- physical or mental health needs
- racial or ethnic origin
- criminal convictions data
- civil and criminal proceedings, outcomes and sentences
- religious or other beliefs of a similar nature

The school collects and uses this information

- to support student learning
- to monitor and report on student progress
- to provide appropriate care and guidance
- to assess the quality of our services
- to comply with the law regarding data sharing

The lawful basis on which this information is used

The school collects and uses student information under Article 6 and Article 9 of the GDPR, this enables the school to process information such as assessments, special educational needs requests, Departmental Censuses under the Education Act 1996 and the Education Act 2005, examination results and other such data processes that relate educational data to the individual within the requirements for the school to provide education for the individual.

Collecting student information

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

How do we collect personal data?

Information may be collected in many different ways but predominantly as set out below:
Face to Face

If you attend the school or we visit you, we may collect your personal data.

Telephone calls
Recordings may be used as evidence of the call and for our staff training, monitoring for abusive and quality purposes.

Emails
If you email the school we may keep a record of your email address and the email as evidence of the contact. We are unable to guarantee the security of any email initiated by you and we recommend that you keep the amount of confidential information you send to us via email to a minimum.

CCTV
We have installed CCTV systems on school premises, for the purposes of public, student and staff safety, as well as, crime prevention and detection. Signs are displayed notifying that CCTV is in operation and providing details of who to contact for further information. The school will only disclose CCTV images to others who intend to use the images for the purposes stated above. CCTV images will not be released to the media for entertainment purposes or placed on the internet. Images captured by CCTV will not be kept for longer than necessary.

Storing student data
We hold student data in line with our Data Retention Guidelines set out in appendix 3.

Sharing student information
We share student information with:

- Schools and other educational environments that students attend after leaving the school
- Lincolnshire Education Authority or the local authority in which the student resides
- Department for Education (DfE)
- School Nursing Team
- National Health Service
- Careers Advisory Service
- Educational Welfare Officer
- Educational Psychology Service
- Special Educational Needs and Disability Specialist Services
- Examination Boards
- Please follow the link for an additional list of suppliers who act as Data Controller or Data Processor:
  Copy of List of companies acting as Data Processor and or Data Controller.xlsx

Why the school shares student information
The school does not share information about students with anyone without consent unless the law and school policies allow us to do so.

The school shares student data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

The school is required to share information about students with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

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

Youth support services
Students aged 13+
Once a student reaches the age of 13, the school passes student information to the local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

A parent or guardian can request that **only** their son's name, address and date of birth is passed to their local authority, or provider of youth support services, by informing us. This right is transferred to the student once he reaches the age 16.

Students aged 16+
The school shares certain information about students aged 16+ with the local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:
- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit the local authority website.

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

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

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

The department may share information about students from the NPD with third parties who promote the education or well-being of children in England by:
- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:
- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

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

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data
For information about which organisations the department has provided student information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-student-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to a student's personal data
Under data protection legislation, parents and students have the right to request access to information about them held by the school. To make a request for your personal information, or be given access to your son's educational record, contact Catherine Barnes, Bursar & Director of Resources / Data Protection Officer via: mailto:admin@kings.lincs.sch.uk

You also have the right to:

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

If you have a concern about the way the school is collecting or using your personal data, you should raise your concern with the Head Master in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact
If you would like to discuss anything in this privacy notice, please contact: Catherine Barnes, Bursar & Director of Resources / Data Protection Officer

APPENDIX 3: RETENTION AND DISPOSAL SCHEDULE

1. MANAGEMENT OF THE SCHOOL

This section contains retention periods connected to the general management of the school. This covers the work of the Governing Body, the Head Master and the Senior Leadership Team, the admissions process and operational administration.

1.1 Governing Body	Basic file description	Data Protection 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 staff		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 the Governing Body meetings	There may be data protection issues if the meeting is dealing with confidential issues relating to staff			
	Principal Set (signed)			PERMANENT	
	Inspection Copies [2]			Date of meeting + 3 years	If these minutes contain any sensitive, personal information, they must be shredded
1.1.3	Reports presented to the Governing Body	There may be data protection issues if the report deals with confidential issues relating to staff		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	Instruments of Government including Articles of Association	No		PERMANENT	These should be retained in the school
1.1.5	Trusts and Endowments managed by the Governing Body	No		PERMANENT	These should be retained in the school
1.1.6	Action plans created and administered by the Governing Body	No		Life of the action plan + 3 years	SECURE DISPOSAL
1.1.7	Policy documents created and administered by the Governing Body	No		Life of the policy + 3 years	SECURE DISPOSAL
1.1.8	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
1.1.9	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 SI2002 No 1171	Date of report + 10 years	SECURE DISPOSAL
1.1.10	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 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 Governors 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

1.2 Head Master & Senior Manage-ment Team	Basic file description	Data Protection 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 Master	There may be data protection issues if the log book refers to individual pupils or members of staff		Date of last entry in the book + a minimum of 6 years then review	
1.2.2	Minutes of Senior Leadership Team (SLT) meetings and the meetings of other internal administrative bodies	There may be data protection issues if the minutes refers to individual pupils or members of staff		Date of the meeting + 3 years then review	SECURE DISPOSAL
1.2.3	Reports created by the Head Master or the SLT	There may be data protection issues if the report refers to individual pupils or members of staff		Date of the report + a minimum of 3 years then review	SECURE DISPOSAL
1.2.4	Records created by the Head Master, Deputy Headmasters, Assistant Headteachers, Subject Leaders, Heads of Year and other members of staff with administrative responsibilities	There may be data protection issues if the records refer to individual pupils or members of staff		Current academic year + 6 years then review	SECURE DISPOSAL
1.2.5	Correspondence created by Head Master, Deputy Headmasters, Assistant Headteachers, Subject Leaders , Heads of Year and other members of staff with administrative responsibilities	There may be data protection issues if the correspondence refers to individual pupils or members of staff		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 Improvement Plans	No		Life of the plan + 3 years	SECURE DISPOSAL
1.2.8	Parental Questionnaire	Yes		Within the academic year collected + 1 year	SECURE DISPOSAL
1.2.9	Student Questionnaire	Yes		Within the academic year collected + 1 year	SECURE DISPOSAL
1.2.10	Staff Questionnaire	Yes		Within the academic year collected + 1 year	SECURE DISPOSAL

1.3 Admissions Process	Basic file description	Data Protection 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, school adjudicators and admission appeals panels December 2014	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 2014	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 2014	Every entry in the admission register must be preserved for a period of three years after the date on which the entry was made	The admission register will be kept permanently as the school occasionally receives enquiries from past student 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	Proof 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 2014	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	Yes		This information should be added to the student file	SECURE DISPOSAL
	For unsuccessful admissions	Yes		Until appeals process is completed	SECURE DISPOSAL

1.4 Operational Information	Basic file description	Data Protection 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 students	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

2. HUMAN RESOURCES

2.1 Recruitment	Basic file description	Data Protection 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
2.1.3	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 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 2014: Keeping children safe in education (statutory guidance from DoE)	The school does not have to keep copies of DBS certificates	
2.1.5	Proofs of identity collected as part of the process of checking 'portable' enhanced DBS disclosure	Yes		These should be checked and a note kept of what was seen and what has been checked. If it is felt necessary to keep 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	Yes	An employer's guide to right to work checks (Home Office)	Where possible these documents should be added to the staff personal file but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than 2 years	

2.2 Operational Staff Management	Basic file description	Data Protection 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 & Grievance Processes	Basic file description	Data Protection 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	Yes	"Keeping children safe in education Statutory guidance for schools and colleges", "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children	Until the person's normal retirement age or 10 years from the date of the allegation whichever is the longer then REVIEW. Note allegations that are found to be malicious should be removed from personnel files. If found they are to be kept on the file and a copy provided to the person concerned	SECURE DISPOSAL These records must be shredded
2.3.2	Disciplinary Proceedings Oral warning Written warning – level 1 Written warning – level 2 Final warning Case not found	Yes Yes Yes Yes Yes Yes		 Date of warning + 6 months Date of warning + 6 months Date of warning + 12 months Date of warning + 18 months If the incident is child protection related then see above, otherwise dispose of at the conclusion of the case	 SECURE DISPOSAL (if warnings are placed on personal files then they must be weeded from the file) SECURE DISPOSAL

2.4 Health & Safety	Basic file description	Data Protection 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 Adults Children	Yes	Social Security (Claims & Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	 Date of the incident + 6 years DOB of the child + 25 years	 SECURE DISPOSAL 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 & Pensions	Basic file description	Data Protection 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 (S11 986/1960), revised 1999 (S11 999/567)	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 & Insurance	Basic file description	Data Protection 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 Protection 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 & Statements including Budget Management	Basic file description	Data Protection 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 Protection 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 years	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 Protection 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 Protection 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

4.1 Property Management	Basic file description	Data Protection 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 Protection 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. STUDENT MANAGEMENT

5.1 Student's Educational Record	Basic file description	Data Protection Issues	Statutory Provisions	Retention Period (Operational)	Action at the end of the administrative life of the record
5.1.1	Student's Educational Record required by The Education (Pupil Information) (England) Regulations 2005 Secondary	Yes	The Education (Pupil Information) (England) Regulations 2005 SI 2005 No 1437 Limitation Act 1980 (Section 2)	Date of Birth of the student + 25 years	SECURE DISPOSAL
5.1.2	Examination Results – Student Copies Public Internal	Yes	This information should be added to the student file This information should be added to the student file		All uncollected certificates should be returned to the examination board
5.1.3	Child Protection information held on student file	Yes	"Keeping children safe in education Statutory guidance for schools and colleges". "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	If any records relating to child protection issues are placed on the student file, it should be in a sealed envelope and then retained for the same period of time as the student 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 for schools and colleges". "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children"	DOB of the child + 25 years 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

5.2 Attendance	Basic file description	Data Protection 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 3 years after the date on which the entry was made	SECURE DISPOSAL
5.2.2	Correspondence relating to authorised absence		Education Act 1996 Section 7	Current academic year + 2 years	SECURE DISPOSAL

5.3 Special Educational Needs	Basic file description	Data Protection 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 student + 25 years	REVIEW: NOTE: This retention period is the minimum retention period that any student 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 student + 25 years (this would normally be retained on the student 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 student + 25 years (this would normally be retained on the student file)	SECURE DISPOSAL unless the document is subject to a legal hold
5.3.4	Accessibility Strategy	Yes	Special Education Needs and Disability Act 2001 Section 14	Date of birth of the student + 25 years (this would normally be retained on the student 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 Protection 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	
6.1.2	Examination Results (Schools Copy) SATS records Results Examination papers	Yes Yes		Current year + 6 years The SATS results should be recorded on the student's educational file and will therefore be retained until the student 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 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 Protection 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	
6.2.3	Mark Books	Yes		Current year + 1 year	
6.2.4	Record of homework set	No		Current year + 1 year	
6.2.5	Student's Work	No		Where possible student's work should be returned to the student 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 Protection 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 – 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
7.1.2	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 issued by the school for this period of time
7.1.3	Parental permission slips for school trips – where there has been a major incident	Yes	Limitation Act 1980 (Section 2)	Date of Birth of the student involved in the incident + 25 years. The permission slips for all students on the trip need to be retained to show that the rules had been followed for all students	

8. CENTRAL GOVERNMENT AND LINCOLNSHIRE AUTHORITY

8.1 Central Government & Local Authority	Basic file description	Data Protection 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 Protection 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

APPENDIX 4: SUBJECT ACCESS REFERRAL FORM

The General Data Protection Regulations (GDPR) provides each employee or student, the data subject, with the right to receive a copy of the data /information the school holds about them, or to authorise someone to act on their behalf. This form should be completed if the subject wishes to see their data. The Subject will need to provide **proof of identity**. The request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of identity:
Proof of identity must include a copy of two acceptable documents such as birth certificate, passport, driving license, official letter containing the name of the subject and their address e.g. bank statement, recent utilities bill or council tax bill. The documents should include the subject's name, date of birth and current address. If the subject has changed their name, please supply relevant documents evidencing the change.

Administration fee:
There is no charge for Subject Access Requests.

Section 1
Please fill in your details (the data subject). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other ☐ **Surname/Family Name:**		
First Name(s)/Forenames:		
Date of Birth:		
Address: **Post Code:**		
Previous Addresses: **Post Code:**		
Daytime Telephone Number(s):		

I am enclosing the following copies as proof of identity:

Birth certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐

Personal Information

If you only want to know what information is held in specific records please indicate in the box below.
Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records ☐

If you are now, or have been employed by The King's School and are seeking personal information in relation to your employment, please provide details of your payroll number/and dates of employment:

Payroll number: ……

Dates of employment:
From: …… To: …….

Section 2

If you are NOT the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other ☐
Surname/Family Name:
First Name(s)/Forenames:
Date of Birth:
Address: **Post Code:**
Daytime Telephone Number(s):

Please provide proof of identity as detailed on page 1

I am enclosing the following copies as proof of identity: Birth certificate ☐ Driving Licence ☐ Passport ☐ An official letter to my address ☐

What is your relationship to the data subject? (e.g. parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:	
Letter of authority ☐	Lasting or Enduring Power of Attorney ☐
Evidence of parental responsibility ☐	Other (give details):

Data Subject Declaration I certify that the information provided on this form is correct to the best of my knowledge and that I am the person to whom it relates. I understand that The King's School is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.
Name:
Signature: **Date:**
OR
Authorised person – Declaration (if applicable): I confirm that I am legally authorised to act on behalf of the data subject. I understand that The King's School is obliged to confirm proof of identity/authority and it may be necessary to obtain further information in order to comply with this subject access request.
Signature: **Date:**
Warning: A person who unlawfully obtains or attempts to obtain data is guilty of a criminal offence and is liable to prosecution

I wish to:

Receive the information in electronic format ☐
(some files may be too large to transmit electronically and we may have to supply in CD format)

Receive the information by post*	☐	Collect the information in person	☐
View a copy of the information only of staff	☐	Go through the information with a member of staff	☐

* Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity to:

Catherine Barnes
Data Protection Officer
The King's School
Brook Street
Grantham
Lincolnshire
NG31 6RP

admin@kings.lincs.sch.uk

The King's School will retain the information provided and only share the information with those it is legally entitled to. The information will only be kept for as long as necessary and in accordance with The King's School Retention Policy, will be disposed of in a safe and secure manner.

APPENDIX 5 - PERSONAL DATA BREACH PROCEDURE

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the member of staff or data processor must notify Catherine Barnes (DPO).
- The DPO will investigate the report and determine whether a breach has occurred. The DPO will consider whether personal data has been accidentally or unlawfully: lost, stolen, destroyed, altered, disclosed or made available where it should not have been or made available to an unauthorised person.
- The DPO will inform the Head Master and the Chair of Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by the relevant staff members or data processors, where appropriate.
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identity theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned.

- The DPO will document the decision in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. The DPO will set out:

  - A description of the nature of the personal data breach including where possible the categories and approximate numbers of individuals concerned; the categories and approximate number of personal data records concerned.
  - The name and the contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are now yet known the DPO will report as much as possible within 72 hours. The report will explain that there is a delay, the reasons for it, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.
- The DPO will assess the risk to individuals based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will inform, in writing, all individuals whose personal data has been breached. This notification will set out:

  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The DPO will notify any relevant third parties who can help mitigate the loss to individuals for example; the police, insurers, banks or credit card companies.
- The DPO will document each breach, irrespective of whether it is reported to the ICO. The record will include: the facts and cause, effects and action taken to contain the breach to ensure it does not happen again.
- The DPO and Head Master will meet as soon as possible to review what happened and how it can be stopped from happening again.

APPENDIX 6 - CLEAN DESK & CLEAR SCREEN PROCEDURE

CLEAN DESK PROCEDURE

- Personal confidential information must not be left unattended. Ideally, all staff should leave their desk paper free at the end of the day.
- Ensure that you select an appropriately located printer where you are able to retrieve your printing immediately. Do not leave personal confidential information for others to find.
- An easy way to comply with the clear desk procedure is to work with electronic documents whenever possible – "do you need to print it"?
- Ensure documents are disposed of securely. Never put documents containing sensitive, personal or corporate sensitive information in the general waste bins. Use the confidential paper shredding boxes.
- All Portable Computing & Data Storage Devices (PCDs) such as USB data sticks, mobile phones and laptops should be placed out of sight, preferably locked away at the end of the working day.

CLEAR SCREEN PROCEDURE

- Always lock the desktop when leaving the workstation/desk unattended. If using a shared workstation/desk it may be more appropriate to use the 'switch user' function rather than logging off. If anticipating an absence of 30 minutes or more log off or shutdown the computer. This also applies when using a laptop.
- Pressing CTRL+ALT+DEL and clicking 'Lock this computer' is straight forward and simple. However, a windows key combination is even simpler. Press windows key + L and your computer will lock automatically. (The windows key can usually be found in the bottom left of the keyboard and looks like a flag/window.)
- To unlock press CTRL+ALT+DEL and log back in.
- Always be aware of the position of the screen on your workstation. Wherever possible, ensure that it cannot be seen by unauthorised people while in use.