LEVEN CE (VC) PRIMARY SCHOOL
Data Protection Policy

Effective Date:	**25th May 2018**
Date Reviewed:	**22nd May 2018**
Date Due for Review:	**22nd May 2019**
Contact Officer:	**DPO – Anne Tennison**
Approved By:	**Leven CE (VC) Primary School Governing Body**

1. Background

The Data Protection Act 2018 (DPA 2018) makes provision for the General Data Protection Regulation (GDPR) 2016 and the EU Crime Directive 2016 in to UK law. The DPA 2018 replaces the Data Protection Act 1998, superseding the laws developed in compliance with the Data Protection Directive 95/46/EC. The purpose of the updated data protection legislation[1] is to protect the 'rights and freedoms' of natural persons (i.e. living individuals) and to ensure that personal data is not processed without their knowledge.

Data protection legislation applies to all data controllers that are established in the UK, who process the personal data of data subjects. It will also apply to data controllers outside of the UK that process personal data in order to offer goods and services, or monitor the behaviour of data subjects who are resident in the UK.

The Information Commissioner oversees compliance and promotes good practice, regulating all organisations and individuals who process personal data. This Data Protection Policy applies to all personal data held by LEVEN CE (VC) PRIMARY SCHOOL. The policy aims to ensure those individuals' rights and freedoms are protected, preventing personal data being mistreated or used to deny access to services. The policy will be used to ensure that the personal data the Leven CE (VC) Primary Schoolholds is used fairly and lawfully, in line with data protection legislation.

This policy will be reviewed on an annual basis to ensure that it reflects changes to existing legislation, and any new legislation.

2. Definitions for the Purposes of this Policy

For the purposes of this policy, the following definitions are in relation to Data Protection.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the

[1] "The data protection legislation" means—
(a) the GDPR, including the applied GDPR,
(b) DPA 2018, including regulations made under DPA 2018, and
(c) regulations made under section 2(2) of the European Communities Act 1972 which relate to the GDPR or the Law Enforcement Directive.

physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data subject – any living individual who is the subject of personal data held by an organisation.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Personal data breach (PDB) – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the Information Commissioners Office (ICO) and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Child – anyone under the age of 13 years old. The processing of personal data of a child for online services[2] are only lawful if parental or custodian consent has been obtained (this does not include preventive or counselling services). The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

Consent - in relation to the processing of personal data relating to an individual, means a freely given, specific, informed and unambiguous indication of the individual's wishes by which the individual, by a statement or by a clear affirmative action, signifies agreement to the processing of the personal data.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

[2] Refers to information society services as defined by the Electronic Commerce Regulations 2002

3. Policy Statement

In order to operate effectively, Leven CE (VC) Primary School has to process personal information about people with whom it works. These may include members of the pupils, parents, current, past and prospective employees and suppliers. In addition, it is required by law to process information in order to comply with the requirements of central government.

Leven CE (VC) Primary School is committed to ensuring compliance with data protection legislation. Leven CE (VC) Primary School regards the lawful and correct treatment of personal information as essential to its successful operations and to maintaining confidence between Leven CE (VC) Primary School and those with whom it carries out business. Leven CE (VC) Primary School fully endorses the principles of data protection by design and default. To this end, Leven CE (VC) Primary School will ensure its Data Protection Officer is able to fulfil their tasks as defined in data protection legislation.

Third parties who have access to personal data will be expected to have read and understood this policy. No third party will be able to access personal data without being committed to having obligations no less onerous than Leven CE (VC) Primary School. Leven CE (VC) Primary School will make every effort to ensure data subjects can exercise their rights. Any breach of data protection legislation will be dealt with as a matter of urgency. **If required, breaches will be reported to the appropriate authorities and dealt with as criminal offence.** Leven CE (VC) Primary School is committed to working with the ICO in all areas relating to personal data.

4. Corporate Requirements

Leven CE (VC) Primary School is a data controller as defined by data protection legislation. It is the responsibility of the Governors to ensure compliance with Data Protection legislation. However the Head Teacher is responsible for ensuring compliance within the day to day activities of the school.

All those in managerial or supervisory roles throughout the Leven CE (VC) Primary School are responsible for encouraging good information handling practices. Compliance with data protection legislation and this policy is the responsibility of all employees.

Employees are responsible for ensuring that any personal data about them and supplied by them is accurate and up-to-date. **All employees who process personal data are responsible for their own compliance with data protection legislation and this policy. Failure to do so may result in disciplinary action which could lead to dismissal.** Leven CE (VC) Primary School's Training Procedure sets out the specific training requirements and awareness raising requirements.

Leven CE (VC) Primary School appointed Data protection Officer (DPO) is accountable to the Headteacher and will ensure that the tasks outlined within data protection legislation are fulfilled. The DPO carries out their tasks for the following schools:

- Leven CE (VC) Primary School.

The first point of contact for data protection matters is the Headteacher; however anyone has the right to speak to the DPO about their tasks.

5. Policy Development including Consultation

The following people and groups were consulted in development of this policy:

Leven CE (VC) Primary School governing body
East Riding of Yorkshire Council *(as part of a traded service)*
IT Governance Ltd as part of the East Riding of Yorkshire Council's traded service *(this document contains material that is distributed under licence from IT Governance Ltd. No reproduction or distribution of this material is allowed outside of your organisation without the permission of IT Governance Ltd.)*

6. Links with other Policies and Strategies

This policy links to other Leven CE (VC) Primary School documents:

- SEND
- ASSESSMENT
- SOCIAL MEDIA
- CONTINUING PROFESSIONAL DEVELOPMENT
- APPRAISAL
- PAY
- ATTENDANCE AT WORK
- EQUAL OPPORTUNITIES
- COMMUNITY COHESION
- RACE EQUALITY
- INCLUSION
- GIFTED & TALENTED
- CHILD PROTECTION
- SAFEGUARDING
- INITIAL ALLEGATION MANAGEMENT
- ESAFETY & INTERNET USE
- WEBSITE
- GOOD BEHAVIOUR
- BREAKFAST CLUB
- EDUCATIONAL VISITS
- VOLUNTEER HELPERS IN SCHOOL
- PARENTAL INVOLVEMENT
- INDUCTION
- CHARGES & REMISSIONS
- COMPLAINTS
- ABSENCE FROM SCHOOL FOR EXCEPTIONAL CIRCUMSTANCES
- GRIEVANCES
- SENIOR LEADERSHIP TEAM CODE OF CONDUCT
- GOVERNOR HANDBOOK
- STAFF CODE OF CONDUCT

7. Data Protection Principles

All processing of personal data must be conducted in accordance with data protection principles. Leven CE (VC) Primary School's policies and procedures are designed to ensure compliance with these principles.

1. Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – data protection legislation includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

2. Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the ICO, outlined on Leven CE (VC) Primary School records of processing or in line with this Policy.

3. Personal data must be adequate, relevant and limited to what is necessary for processing

The Leven CE (VC) Primary School does not collect information that is not strictly necessary for the purpose for which it is obtained. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the DPO. The DPO will ensure that, on a regular basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive.

4. Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by Leven CE (VC) Primary School must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate. The DPO is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is the responsibility of the data subject to ensure that data held by Leven CE (VC) Primary School is accurate and up to date. Pupils, parents, employees and suppliers should be required to notify Leven CE (VC) Primary School of any changes in circumstance to enable personal records to be updated accordingly. Processes will be in place to allow for the updating of records. It is the responsibility of Leven CE (VC) Primary School to ensure that any notification regarding change of circumstances is recorded and acted upon.

The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date. On a regular basis the DPO will review these processes and retention dates for personal data processed by Leven CE (VC) Primary School.

The DPO is responsible for making appropriate arrangements so that, third-party organisations that may have been passed inaccurate or out-of-date personal data are informed, ensuring it is not used to inform decisions about the individuals concerned.

5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where possible, personal data will be minimised, encrypted or pseudonymised in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention schedule (appendix 1) and, once its retention date is passed, it must be securely destroyed. Any data retention that exceeds the retention period must be approved by the Head Teacher. They must ensure that the justification is clearly identified and in line with the requirements of data protection legislation.

6. Personal data must be processed in a manner that ensures the appropriate security

Leven CE (VC) Primary School will carry out risk assessments taking into account how state of the art technical measures are, the costs of implementation and the risk/likelihood to individuals if a security breach occurs, the effect of any security breach on Leven CE (VC) Primary School itself, and any likely reputational damage including the possible loss of customer trust.

Both Leven CE (VC) Primary School (as controller) and its processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including where appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The policies and strategies identified in Section 6 of this Policy (6. Links with other Policies and Strategies) must also be considered.

7. The controller must be able to demonstrate compliance with the GDPR's other principles (accountability)

Data protection legislation includes provisions that promote accountability and governance. These complement the transparency requirements. This accountability additional principle requires Leven CE (VC) Primary School to demonstrate that it complies with the principles and states explicitly that this is Leven CE (VC) Primary School's responsibility.

Leven CE (VC) Primary School demonstrates this compliance through this policy, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, and establishing formal procedures in relation to data protection.

8. Data Subjects' Rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.
- To request the ICO assess whether any provision of the data protection legislation has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller (ported).
- To object to any automated profiling that is occurring without consent.

Leven CE (VC) Primary School makes every effort to ensure that data subjects may exercise these rights. A data subject may make a data access request as described in the Leven CE (VC) Primary School Process. These requests are under normal circumstances free of charge and will be dealt with in one month (although they can be extended by two months in some circumstances).

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2006 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records. As part of this process the school will apply the appropriate charge for providing copies of records.

Personal data must not be disclosed about a third party except in accordance with data protection legislation. If it appears absolutely necessary to disclose information about a third party, advice should be sought from the DPO.

Data subjects also have the right to complain to Leven CE (VC) Primary School in relation to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled. This will be done in line with Leven CE (VC) Primary School's Complaints Policy.

9. Disclosure of Data

Leven CE (VC) Primary School ensures that personal data is not disclosed to unauthorised third parties which includes family members, friends, suppliers, government bodies and other public sector organisations. All employees should exercise caution when asked to disclose personal data held on another individual to a third party.

All requests to provide data must be supported by the appropriate documentation. Data protection legislation permits disclosures for a number of reasons without consent, these include:

- to safeguard national security;
- prevention or detection of crime including the apprehension or prosecution of offenders;
- assessment or collection of tax duty;
- discharge of regulatory functions (includes health, safety and welfare of persons at work);
- to prevent serious harm to a third party; and
- to protect the vital interests of the individual, this refers to life and death situations.

It is the responsibility of employees to ensure that they have the authority to share information and that the recipient is authorised to receive such information. **Failure to do so could lead to action under Leven CE (VC) Primary School's disciplinary procedure (and, in exceptional circumstances, criminal charges).** Leven CE (VC) Primary School has a framework in place to facilitate information sharing, the Humber Information Sharing Charter.

Advice should always be sought from the DPO if there is any uncertainty around the disclosure of information.

10. Data Transfers

All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate 'level of protection for the fundamental rights of the data subjects'.

The transfer of personal data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

- An adequacy decision.
- Privacy shield.
- Binding corporate rules.
- Model contract clauses.

Exceptions, in the absence of the above a transfer of personal data to a third country or international organisation, shall only take place on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;

- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

11. Consent

Leven CE (VC) Primary School understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be valid.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. The data controller must be able to demonstrate that consent was obtained for the processing operation. For special categories data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Where Leven CE (VC) Primary School provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 13.

Whether or not a photograph needs to be protected or falls under data protection legislation can be open to interpretation and the quality of the photograph. However, the school takes this matter extremely seriously and seeks to obtain parents' consent for the use of photographs outside the school and, in particular, to record their wishes if they do not want photographs to be taken of their children.

12. Processors and Contracts

Leven CE (VC) Primary School will ensure that any processor it engages have a written contract or agreement in place. This is important so both parties understand their responsibilities and liabilities. Processors must only ever act on documented instructions. To be compliant with data protection legislation contracts must include specific items.

13. Retention and Disposal of Data

Leven CE (VC) Primary School will not keep personal data in a form that permits identification of data subjects for longer than is necessary, in relation to the purpose(s) for which it was originally collected. It may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in Leven CE (VC) Primary School retention schedules.

Personal data must be disposed of securely in accordance with data protection principle 6. Appropriate procedures must be followed when disposing of personal information.

Leven CE (VC) Primary School will ensure that secure disposal methods are available to staff.

14. Data Inventory

Leven CE (VC) Primary School has established records of processing activity which help determine the flow of data through the organisation. Leven CE (VC) Primary School is aware of any risks associated with the processing of particular types of personal data and the level of risk to individuals associated with the processing of their personal data.

15. Impact Assessments

Leven CE (VC) Primary School will implement technical and organisational measures to ensure that by default, personal data is processed where necessary. Data protection impact assessments (DPIAs) will be carried out in relation to the processing of personal data, and in relation to processing undertaken by other organisations on behalf of Leven CE (VC) Primary School.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, presents a risk to the rights and freedoms of an individual, Leven CE (VC) Primary School, prior to the processing, will carry out a DPIA. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA, it is clear that Leven CE (VC) Primary School is about to commence processing of personal data that could cause damage and/or distress to the data subjects, or is deemed high risk (including to the reputation of Leven CE (VC) Primary School), the DPIA must be escalated for review to the DPO. The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the ICO.

16. Incidents and Breaches

Leven CE (VC) Primary School will always treat any data protection incident/breach as a serious issue. In the event of a breach, or suspected breach (incident), the DPO must be informed immediately.

An investigation will take place in line with the Leven CE (VC) Primary School's procedures. **This includes Human Resources to ensure any disciplinary action is taken if deemed appropriate and Legal Services.** The point of contact for the ICO is the DPO.

Leven CE (VC) Primary School has an obligation to report certain data protection breaches to the ICO within 72 hours of Leven CE (VC) Primary School being made aware. The DPO will notify the ICO following an assessment of the breach. If required the DPO will also arrange for the affected data subjects to be notified. Any data processors Leven CE (VC) Primary School is working with are also required to report data protection breaches to the ICO, as well as cooperate with the ICO to resolve the issue. Data processors must also notify Leven CE (VC) Primary School of any breach which affects Leven CE (VC) Primary School's personal information, within the 72 hour window.

The ICO has the authority to sanction significant financial penalties of up to €20 million or 4% of global turnover (fines in the UK will be based on the current exchange rate). Data processors also hold liability for data protection breaches.

Leven CE (VC) Primary School recognises data subjects' right to compensation if they have suffered material or non-material damage as a result of an infringement of data protection legislation. Any claim for compensation will be dealt with through Leven CE (VC) Primary School's normal procedures.

17. Risk Management

As part of the Leven CE (VC) Primary School approach to risk management, the following must be adhered to by all staff:

- *Computers screens must be locked with* 

when not in use.
- *All staff must use a school generated email that will be in the form of ad@levenschool.org. This is operated through G Suite for Education. All electronic communications between school and staff, and staff and school will use this email. All official emails from staff to other agencies, parents, governors, and any other organisation or individual that official communications are needed for, will use the official school email.*
- *All governors must use a school generated email that will be in the form of ad@levenschool.org. This is operated through G Suite for Education. All electronic communications between school and governors, and governors and school will use this email. All official emails from governors to other agencies, parents, governors, staff and any other organisation or individual that official communications are needed for, will use the official school email.*
- *Governors will not breach data protection procedures or Governors code of conduct.*
- *All staff will keep a clear desk (i.e. no paper with personal data will be left on the desk)*
- *All staff and governors will follow the Data Protection Breach Procedure when needed*
- *All staff and governors will follow the privacy notice and consent guidance*
- *All staff and governors will follow guidance re: data processors and handling personal data guidance*
- *All staff and governors will follow guidance re: data protection impact assessment procedures*
- *All staff and governors will follow guidance on redaction*
- *All staff and governors will follow data protection request procedures*
- *Sensitive data will be stored in the lockable cupboard in the main office – only the headteacher and the school business manager will have access to this cupboard.*
- *All stored data will have a destroy date attached to it – see appendix 2*
- *If data needs to be taken off the school premises, an encrypted usb stick will be used. Teachers will be provided with an encrypted usb stick. No data will be stored on laptops or on cloud services.*

18. Training

It is the Leven CE (VC) Primary School policy that all employees and processors who have access to Leven CE (VC) Primary School personal data receive the appropriate training, in order to comply with data protection legislation. Leven CE (VC) Primary School will accordingly ensure that data protection training is available for staff.

Training in data protection matters should be provided before any access to personal data is permitted, and mandatory refresher training should be undertaken at intervals thereafter to maintain awareness. The School Business Manager is responsible for ensuring appropriate training has been undertaken, including for temporary or contracted staff.

Data protection training is a crucial element of staff awareness. All individuals need to be aware of their obligations relating to any personal data they process as part of their Leven CE (VC) Primary School duties. **Failure to adhere to this policy can result in serious misconduct and lead to the prosecution of employees.**

19. Outcomes and Impacts

- Prevent the inappropriate use of personal data held by Leven CE (VC) Primary School.
- Ensure employees are aware of their responsibilities for handling personal data and that failure to do so could result in disciplinary proceedings and in some cases criminal proceedings.
- Ensure services and employees know who to contact for advice.
- Training requirements are identified and staff have the required level of data protection knowledge.
- Uphold data subjects' rights.
- Data processors working on behalf of Leven CE (VC) Primary School are aware of their responsibilities and handle personal data in accordance with this policy.
- Leven CE (VC) Primary School has an appointed DPO and her duties are defined.
- Leven CE (VC) Primary School is compliant with data protection legislation.

20. Evaluation

The Data Protection Policy will be subject to an annual review to ensure that it is appropriate and responsive to all relevant legislation and guidance.

21. References

Data Protection Act 2018
Data Protection Act 1998
https://ico.org.uk/
General Data Protection Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC
Crime Directive - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644827/LED_Document.pdf
https://www.privacyshield.gov/welcome
Human Rights Act 1998
Freedom of Information Act 2000

22. Appendix 1

(Data Protection: a toolkit for schools - Annex 4.1: The possible lawful basis and conditions of processing for personal data)

The lawful basis for processing personal data

These are set out in Article 6 of the General Data Protection Regulation (GDPR). At least one of these must apply whenever you process personal data:
a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

d) Vital interests: the processing is necessary to protect someone's life.

e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. This cannot apply if you are a public authority processing data to perform your official tasks. Public authorities will need to rely on official functions.

Where you are processing special category data, set out in Article 9 of GDPR, as well as one of the six lawful basis for processing, you must ensure that a condition for processing from the following list applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.

b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the

processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

e) processing relates to personal data which are manifestly made public by the data subject.

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Schools will also need to know and rely upon the additional conditions for processing special category in Schedule One of the Data Protection Bill, when finalised.

23. APPENDIX 2

(Data Protection: a toolkit for schools - Annex 5.1 An Emerging Data Retention Strategy for the sector)

Data item group	Short term need (event +1 month)	Medium term need (pupil at school +1 year)	Medium term need (pupil at school +3 years)	Long term need (pupil at school +5 years)	Very long term need (until the pupil is aged 25 or older)	+ 6 years	+ 10 years	Operational	Permanent	Justification
Admissions		X (admissions files)		X (admissions appeals)						**Admissions files** Admissions data is used extensively from the period of the school receiving it up until the point where children enrol. It is then used for some validation and cross checking of enrolment details. Once enrolled, the child's records in the MIS become the core record. Data about children who enrolled but didn't get in is useful, but any intelligence gathered from it (for example, where in the city children are interested in our school, or the SEN make up) is aggregated within the first year to a level being non-personal, after that, the detailed data within the admission file could be deleted. It is important to retain detailed data for a year, any appeals for which richer data about other successful/unsuccessful appeals may be relevant typically happen in the first year. **Information about admissions appeals** When dealing with appeals, having a reasonable history of any other appeals in some detail can be needed to deal with the particular appeal. The information is needed alongside the admissions policies of the time.
Attainment				X						**Formative assessment** data is useful as a child is building towards a particular more formal assessment. Once the child leaves the school, it has little value in terms of retention. **Summative attainment** is the main outcome of what children 'attain' in school. It is important that future schools where pupils go on to learn can understand previous attainment. Whilst often that information is 'passed on' smoothly as children move phase, it is not always the case, and thus retaining the names alongside the main attainment data for 1 year after the pupil has left the school feels proportionate. **Trend analysis** is important, 3 to 5 years is often the 'trend' people look at, but longer may be relevant. Whilst this must be fully flexible in reporting small sub groups, and the data would wish to be retained at individual level, some personal data (for example, name) could be removed from the data to reduce sensitivity. After 3 to 5 years, then aggregated summaries that have no risk of identifying individuals are all that are typically needed to be retained.
Attendance		X								Attendance data probably resides in some 'operational' systems in schools, such as cashless catering. In these systems, the data should only be retained until the associated business processes have concluded (for example, payment of meals). The start of the next academic year once all bills are settled feels proportionate. Attendance is related to individual attainment and so being able to relate attendance to attainment whilst in our care is important. Keeping it in detailed, individual form for one year after the pupil leaves school support conversations about detailed attendance that may be needed to best support that child. After that period, non-identifiable summary statistics are all that is required to support longer term trend analysis of attendance patterns. We noted another GDPR principle here that may apply to attendance. Under data minimisation, where 'paper records' capture attendance, this paper record duplicates the electronic version and is probably not required once the paper has been transferred to a stable electronic format.
Behaviour		X								This is all relevant for managing children when with at your school. 1 year allows a period of 'handover' to next institution with conversations supported by rich data if relevant.
Exclusions		X								Exclusion data should be 'passed on' to subsequent settings. That school then has responsibility for retaining the full history of the child. If a private setting or the school is unsure on where the child has gone, then the school should ensure the LA already has the exclusion data.
Identity management and	X (images									

authentication	used for identity management)									
Catering and free school meal management		X (meal administration)		X (free school meal eligibility information)						A short historic record of what a child has had may be useful in case of any food-related incidents at school, or parental queries about the types of meals their children are choosing. Keeping for up to one year also allows time to do accounting work associated with catering. Typically 'one month' may not be enough, but 'one year' feels enough. Due to the way school funding works, free school meal eligibility is a financial matter, and thus keeping this data for 6+1 feels appropriate. This 7 - year record also needs to be portable with the pupil, as historic dates can be used for funding.
Trips and activities	X (field file) X (educational visitors into school)			X (financial information related to trips)	X (major medical events)					**Financial information** related to trips should be retained for 6 years + 1 for audit purposes. This would include enough child identifiers to be able to confirm contributions. A **'field file'** is the information that is taken on a trip by a school. This can be destroyed following the trip, once any medicines administers on the trip have been entered onto the core system. If there is a minor medical incident (for example, a medical incident dealt with by staff in the way it would be dealt with 'within school') on the trip, then adding it into the core system would be done. If there is a **major incident** (for example, a medical incident that needed outside agency) then retaining the entire file until time that the youngest child becomes 25 would be appropriate. Permission to go on the trip slips will contain personal data, and destroying them after the trip unless any significant incident arises is appropriate, otherwise refer to the policies above. Schools sometimes share personal data with people providing 'educational visits' into school. There should be good policies in place to ensure that the sharing is proportionate and appropriately deleted afterwards.
Medical information and administration	X (permission slips)	X (medical conditions and ongoing management)			X medical incidents (potentially)					To support any handover work about effective management of medical conditions to a subsequent institution. Permission forms that parents sign should to be retained for the period that medication is given, and for 1 month afterwards if no issue is raised by child/parent. If no issue is raised in that time, that feels a reasonable window to assume all was administered satisfactorily. Adding this policy to the permission slip would seem prudent. Medical 'incidents' that have a behavioural or safeguarding angle (including the school's duty of care) should refer to the retention periods associated with those policies.
Safeguarding					X					All data on the safeguarding file potentially forms part of an important story that may be needed retrospectively for many years. The elements of a pupil file (name, address) that are needed to identify children with certainty are needed to be retained along with those records.
Special educational needs				X						
Personal identifiers, contacts and personal characteristics	X (images used in identity systems) X (biometrics) X (house number and road)	X (images used in displays in school)		X (postcodes) X (names) X (characteristics)						**Images** are used for different reasons, and the reason should dictate the retention period. Images used purely for identification can be deleted when the child leaves the setting. Images used in displays etc. can be retained for educational purposes whilst the child is at the school. Other usages of images (for example, marketing) should be retained for and used in line with the active informed consent captured at the outset of using the photograph. **Biometric data** (typically fingerprints used in things like catering) should be used and retained as set out in the active informed consent gained at the outset, but typically this should not be retained long after the activity that requested its use has finished (for example, the child no longer attends the school to have a meal). As set out in other sections, **names** are needed for smooth handover to subsequent schools for up to one year. **Postcode** data is useful in analysing longer-term performance trends or how catchment/pupil populations are shifting over time, but full address data (house number and road) is not required for that activity. Schools may well provide **references** for pupils for up to 3 years after they leave, and so retaining the name in the core pupil record is important (this doesn't mean it needs to be retained in all systems). Keeping names attached to safeguarding files for longer than this may be entirely appropriate – see safeguarding section.

										Characteristics form an essential part of trend analysis, and so retention is in line with those needs.
Agendas for Governing Body meetings								X		There may be data protection issues if the meeting is dealing with confidential issues relating to staf
Minutes of Governing Body meetings T								X		There may be data protection issues if the meeting is dealing with confidential issues relating to staf
Principal Set (signed)									X	If the school is unable to store these then they should be offered to the County Archives Service
Inspection Copies			X							If these minutes contain any sensitive, personal information they must be shredded.
Reports presented to the Governing Body									X	There may be data protection issues if the report deals with confidential issues relating to staff SECURE DISPOSAL or retain with the signed set of the minutes 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
Meeting papers relating to the annual parents' meeting held under section 33 of the Education Act 2002						X				Date of the meeting + a minimum of 6 years SECURE DISPOSAL
Instruments of Government including Articles of Association									X	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
Trusts and Endowments managed by the Governing Body									X	These should be retained in the school whilst the school is open and then offered to County Archives Service when the school closes.
Action plans created and administered by the Governing Body			X							Life of the action plan + 3 years SECURE DISPOSAL
Policy documents created and administered by the Governing Body			X							Life of the action plan + 3 years SECURE DISPOSAL
Records relating to complaints dealt with by the Governing Body						X				Date of the resolution of the complaint + a minimum of 6 years then review for further retention in case of contentious disputes SECURE DISPOSAL
Annual Reports created under the requirements of the Education (Governor's Annual Reports) (England) (Amendment) Regulations 2002							X			Date of report + 10 years SECURE DISPOSAL
Proposals concerning the change of status of a maintained school including Specialist Status Schools and Academies			X							Date proposal accepted or declined + 3 years SECURE DISPOSAL
Log books of activity in the school maintained by the Head Teacher						X				Log books of activity in the school maintained by the Head Teacher Date of last entry in the book + a minimum of 6 years then review These could be of permanent historical value and should be offered to the County Archives Service if appropriate
Minutes of Senior Management Team meetings and the meetings of other internal administrative bodies			X							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

Reports created by the Head Teacher or the Management Team			X							There may be data protection issues if the report refers to individual pupils or members of staff Date of the meeting + 3 years then Review SECURE DISPOSAL
Records created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities						X				There may be data protection issues if the report refers to individual pupils or members of staff Date of the meeting + 6 years then Review SECURE DISPOSAL
Correspondence created by head teachers, deputy head teachers, heads of year and other members of staff with administrative responsibilities			X							There may be data protection issues if the report refers to individual pupils or members of staff Date of the meeting + 3 years then Review SECURE DISPOSAL
Professional Development Plans						X				Life of the plan + 6 years SECURE DISPOSAL
School Development Plans			X							Life of the plan + 6 years SECURE DISPOSAL
All records relating to the creation and implementation of the School Admissions' Policy			X							School Admissions Code Statutory guidance for admission authorities, governing bodies, local authorities, schools adjudicators and admission appeals panels December 2014 Life of the policy + 3 years then Review SECURE DISPOSAL
Admissions – if the admission is successful		X								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
Admissions – if the appeal is unsuccessful		X								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
Register of Admissions			X							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. REVIEW Schools may wish to consider keeping the admission register permanently as often schools receive enquiries from past pupils to confirm the dates they attended the school.
Proofs of address supplied by parents as part of the admissions process		X								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
Supplementary Information form including additional information such as religion, medical conditions etc For successful admissions								X		This information should be added to the pupil file SECURE DISPOSAL
Supplementary Information form including additional information such as religion, medical conditions etc For unsuccessful admissions								X		Until appeals process completed SECURE DISPOSAL
General file series				X						Current year + 5 years then REVIEW SECURE DISPOSAL

Records relating to the creation and publication of the school brochure or prospectus			X							Records relating to the creation and publication of the school brochure or prospectus STANDARD DISPOSAL
Records relating to the creation and distribution of circulars to staff, parents or pupils		X								Current year + 1 year STANDARD DISPOSAL
Newsletters and other items with a short operational use		X								Current year + 1 year STANDARD DISPOSAL
Visitors' Books and Signing in Sheets						X				Current year + 6 years then REVIEW SECURE DISPOSAL
Records relating to the creation and management of Parent Teacher Associations and/or Old Pupils Associations						X				Current year + 6 years then REVIEW SECURE DISPOSAL
All records leading up to the appointment of a new headteacher						X				Date of appointment + 6 years SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – unsuccessful candidates								X		Date of appointment of successful candidate + 6 months SECURE DISPOSAL
All records leading up to the appointment of a new member of staff – successful candidate								X		All the relevant information should be added to the staff personal file (see below) and all other information retained for 6 months SECURE DISPOSAL
Pre-employment vetting information – DBS Checks								X		DBS Update Service Employer Guide June 2014: Keeping children safe in education. July 2015 (Statutory Guidance from Dept. of Education) Sections 73, 74 The school does not have to keep copies of DBS certificates. If the school does so the copy must NOT be retained for more than 6 months
Proofs of identity collected as part of the process of checking "portable" enhanced DBS disclosure								X		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
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom4								X		An employer's guide to right to work checks [Home Office May 2015] Where possible these documents should be added to the Staff Personal File [see below], but if they are kept separately then the Home Office requires that the documents are kept for termination of Employment plus not less than two years
Staff Personal File							X			Limitation Act 1980 (Section 2) Termination of Employment + 6 years SECURE DISPOSAL
Timesheets							X			Current year + 6 years SECURE DISPOSAL
Annual appraisal/ assessment records				X						Current year + 5 years SECURE DISPOSAL
Allegation of a child protection nature against a member of staff including where the allegation is unfounded								X		"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015" 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
Disciplinary Proceedings oral warning								X		Date of warning + 6 months SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings written warning – level 1								X		Date of warning + 6 months SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings written warning – level 2		X								Date of warning + 12 months SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]
Disciplinary Proceedings final warning								X		Date of warning + 18 months SECURE DISPOSAL [If warnings are placed on personal files then they must be weeded from the file]

Disciplinary Proceedings case not found										If the incident is child protection related then see above otherwise dispose of at the conclusion of the case SECURE DISPOSAL
Health and Safety Policy Statements			X							Life of policy + 3 years SECURE DISPOSAL
Health and Safety Risk Assessments			X							Life of risk assessment + 3 years SECURE DISPOSAL
Records relating to accident/ injury at work								X		Date of incident + 12 years In the case of serious accidents a further retention period will need to be applied SECURE DISPOSAL
Accident Reporting Adults						X				Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 Date of the incident + 6 years SECURE DISPOSAL
Accident Reporting Children					X					Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980 DOB of the child + 25 years SECURE DISPOSAL
Control of Substances Hazardous to Health (COSHH)									X	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
Process of monitoring of areas where employees and persons are likely to have become in contact with asbestos									X	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19 Last action + 40 years SECURE DISPOSAL
Process of monitoring of areas where employees and persons are likely to have become in contact with radiation									X	Last action + 50 years SECURE DISPOSAL
Fire Precautions log books						X				Current year + 6 years SECURE DISPOSAL
Maternity pay records			X							Statutory Maternity Pay (General) Regulations 1986 (SI1986/1960), revised 1999 (SI1999/567) Current year + 3 years SECURE DISPOSAL
Records held under Retirement Benefits Schemes (Information Powers) Regulations 1995						X				Current year + 6 years SECURE DISPOSAL
Employer's Liability Insurance Certificate									X	Closure of the school + 40 years SECURE DISPOSAL
Inventories of furniture and equipment						X				Current year + 6 years SECURE DISPOSAL
Burglary, theft and vandalism report forms						X				Current year + 6 years SECURE DISPOSAL
Annual Accounts						X				Current year + 6 years STANDARD DISPOSAL
Loans and grants managed by the schoo								X		Date of last payment on the loan + 12 years then REVIEW SECURE DISPOSAL
All records relating to the creation and management of budgets including the Annual Budget statement and background papers			X							Life of the budget + 3 years SECURE DISPOSAL
Invoices, receipts, order books and requisitions, delivery notices						X				Current financial year + 6 years SECURE DISPOSAL
Records relating to the collection and banking of monies						X				Current financial year + 6 years SECURE DISPOSAL
Records relating to the identification and collection of debt						X				Current financial year + 6 years SECURE DISPOSAL
All records relating to the management of								X		Limitation Act 1980 Last payment on the contract + 12 years SECURE DISPOSAL

contracts under seal										
All records relating to the management of contracts under signature						X				Limitation Act 1980 Last payment on the contract + 6 years SECURE DISPOSAL
Records relating to the monitoring of contracts								X		Current year + 2 years SECURE DISPOSAL
Free School Meals Registers						X				Current year + 6 years SECURE DISPOSAL
School Meals Registers			X							Current year + 3 years SECURE DISPOSAL
School Meals Summary Sheets			X							Current year + 3 years SECURE DISPOSAL
Title deeds of properties belonging to the school									X	PERMANENT These should follow the property unless the property has been registered with the Land Registry
Plans of property belong to the school								X		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.
Leases of property leased by or to the school						X				Expiry of lease + 6 years SECURE DISPOSAL
Records relating to the letting of school premises						X				Current financial year + 6 years SECURE DISPOSAL
All records relating to the maintenance of the school carried out by contractors						X				Current year + 6 years SECURE DISPOSAL
All records relating to the maintenance of the school carried out by school employees including maintenance log books						x				Current year + 6 years SECURE DISPOSAL
Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005 Primary								X		Pupil's Educational Record required by The Education (Pupil Information) (England) Regulations 2005 Retain whilst the child remains at the primary school The file should follow the pupil when he/she leaves the primary school. This will include: • to another primary school • to a secondary school • to a pupil referral unit • If the pupil dies whilst at primary school the file should be returned to the Local Authority to be retained for the statutory retention period. If the pupil transfers to an independent school, transfers to home schooling or leaves the country the file should be returned to the Local Authority to be retained for the statutory retention period. Primary Schools do not ordinarily have sufficient storage space to store records for pupils who have not transferred in the normal way. It makes more sense to transfer the record to the Local Authority as it is more likely that the pupil will request the record from the Local Authority
Examination Results – Pupil Copies Public									X	This information should be added to the pupil file All uncollected certificates should be returned to the examination board.
Examination Results – Pupil Copies Internal									X	This information should be added to the pupil file
Child Protection information held on pupil file									X	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015" If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file. SECURE DISPOSAL – these records MUST be shredded
Child protection information held in separate files									X	"Keeping children safe in education Statutory guidance for schools and colleges March 2015"; "Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children March 2015" 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
Special Educational Needs									X	Limitation Act 1980 (Section 2) Date of Birth of the pupil + 25 years REVIEW

files, reviews and Individual Education Plans										NOTE: This retention period is the minimum retention period that any pupil file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented.
Statement maintained under section 234 of the Education Act 1990 and any amendments made to the statement									X	Education Act 1996 Special Educational Needs and Disability Act 2001 Section 1 Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] SECURE DISPOSAL unless the document is subject to a legal hold
Advice and information provided to parents regarding educational needs									X	Special Educational Needs and Disability Act 2001 Section 2 Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] SECURE DISPOSAL unless the document is subject to a legal hold
Accessibility Strategy									X	Special Educational Needs and Disability Act 2001 Section 14 Date of birth of the pupil + 25 years [This would normally be retained on the pupil file] SECURE DISPOSAL unless the document is subject to a legal hold
Curriculum returns			X							Current year + 3 years SECURE DISPOSAL
SATS records – Results									X	The SATS results should be recorded on the pupil's educational file and will therefore be retained until the pupil reaches the age of 25 years. The school may wish to keep a composite record of all the whole year SATs results. These could be kept for current year + 6 years to allow suitable comparison SECURE DISPOSAL
SATS records – Examination Papers								X		The examination papers should be kept until any appeals/validation process is complete SECURE DISPOSAL
Published Admission Number (PAN) Reports						X				Current year + 6 years SECURE DISPOSAL
Value Added and Contextual Data						X				Current year + 6 years SECURE DISPOSAL
Self Evaluation Forms						X				Current year + 6 years SECURE DISPOSAL
Schemes of Work		X								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
Timetable		X								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
Class Record Books		X								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
Mark Books		X								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
Record of homework set		X								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
Pupils' Work		X								Where possible pupils' work should be returned to the pupil at the end of the academic year if this is not the school's policy then current year + 1 year SECURE DISPOSAL

24. APPENDIX 3

(Data Protection: a toolkit for schools - Annex 1: Explaining the language around data protection)

Term	Description	Example
Data subject	The person that the data relates to.	John Smith the pupil. Jane Smith the teacher.
Data item	A single piece of information about a data subject.	"Ethnicity = white British" "Attendance = 97%"
Data item group	A group of data items that are typically captured about the same activity or business process in school. These are also sometimes called data elements or data scope within the data community/sharing agreements schools have with suppliers.	Behaviour management, or catering.
System	A piece of software, computer package or manually managed asset that supports the administration of one or more areas of school life.	Capita SIMS, ParentPay, MyMaths.
System group	An umbrella term to describe the areas of school administration where systems that contain personal level data typically reside.	Core MIS, payments, curriculum tools.
Personal data	Information relating to a natural identifiable person, whether directly or indirectly	John Smith was born on 01/01/1990. The head teacher's salary is £60,000.
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons you need to have to access and process that information. In education, it would also be best practice to treat things like FSM, SEN, and CIN/CLA status as special category data.	Tightly defined as data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, health, trade-union membership, and health or sex life. Data relating to criminal offences is also afforded similar special protection.
(Data) Controller	The organisation who (either alone or in common with other people) determine the purpose for which, and the manner in which data are processed.	A school is often the data controller, sometimes a joint controller with the LA or DfE.
(Data) Processor	A person or organisation who process data on behalf of and on the orders of a controller.	A catering supplier the school uses.
Data audit/data asset register	The assessment of data and its quality, for a specific purpose. Other terms you might hear are data map or information asset log. In this context, we simply want the list of personal data assets that we hold, from which we can go on to place further important information alongside.	
Lawful basis and conditions for processing	These are the specific reasons, set out in law, for which you can process personal data. There is one list for personal data (lawful	"The processing is necessary for administering justice, or for exercising statutory

	basis article 6) and another list for processing special category data (article 9).	or governmental functions." Read the full list.
Data retention	How long you will hold information for to do the processing job you need it for. At the end of a data retention period, processes should be in place to ensure it is properly disposed of.	"We keep parent's phone numbers until 1 month after they leave the school in case of any issues that need resolving (for example, payment or repayment of lunch money) and then it is deleted."
Privacy notice	This is a document that explains to the people you have data about ("data subjects") the data items you hold, what they are used for, who it is passed onto and why, and what rights they have.	DfE publish model privacy notices. https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices
Subject Access Request (SAR)	This is where a person (data subject), requests access to the information you hold about them. Timescales for responding, as well as reasons why you must comply or may refuse, as set out in law. A Subject Access Request is often used to describe "tell me all my data you hold".	"I want to know the attendance data you hold about my son"
Data Protection Impact Assessment (DPIA)	This is a process to consider the implications of some change you are introducing on the privacy of individuals. Assessing privacy at the outset helps you plan consultation/awareness/consent type options from the outset. "Privacy by design" is a term that is used in this space.	You would undertake one of these if introducing a new system to use fingerprinting within catering provision.
Data breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.	Sending a list of pupil names, attainment marks and dates of births to the wrong school.
Automated decision making/profiling	This is when machines/software apply rules to data and determine something about someone based on purely applying those rules. Typically it is the significance of the decision which drives the caution and concern here. Read further information.	"Anyone recorded as attendance >99% will get a voucher for X"

25. APPENDIX 3

(Data Protection: a toolkit for schools - Annex 2.1: Table for identifying personal information to support the initial data map)

	Do we receive personal data?	Do we create personal data?	Do we send personal data?	Do we destroy personal data?
Admissions				
Core management information system				
Curriculum tools				
Payment systems				
Virtual learning environments				
Catering management				
Safeguarding				
Trips and transport				
Uniform, equipment and photographs				
Identity management systems				
Contact/communication systems				
Social care and health interactions				
Statutory returns				
References and education settings you pass children onto				
References and education settings you pass children onto				
Paper records				
Other				

26. APPENDIX 4

Good Practice for Managing E-mail

1. Introduction

These guidelines are intended to assist school staff to manage their e-mail in the most effective way, and must be used in conjunction with your school's policies on the use of ICT. Information about how your e-mail application works is not included in this document.

2. Eight Things You Need to Know About E-mail

E-mail has replaced telephone calls and memos

As communicating by e-mail is quick and easy, many people have replaced telephone conversations and memos with e-mail discussions. However, the language in which e-mail is written is often less formal and more open to misinterpretation than a written

memo or a formal letter. Remember that e-mail should be laid out and formulated to your school's standards for written communications.

E-mail is not always a secure medium to send confidential information

You need to think about information security when you send confidential information by e-mail. The consequences of an e-mail containing sensitive information being sent to an unauthorised person could be a civil penalty of up to £500,000 from the Information Commissioner or it could end up on the front page of a newspaper. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Never put personal information (such as a pupil's name) in the subject line of an e-mail.

E-mail is disclosable under the access to information regimes

All school e-mail is disclosable under Freedom of Information and Data Protection legislation. Be aware that anything you write in an email could potentially be made public.

E-mail is not necessarily deleted immediately

E-mails can remain in a system for a period of time after you have deleted them. You must remember that although you may have deleted your copy of the e-mail, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under the Data Protection Act 1998.

E-mail can form a contractual obligation

Agreements entered into by e-mail can form a contract. You need to be aware of this if you enter into an agreement with anyone, especially external contractors. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so.

E-mail systems are commonly used to store information which should be stored somewhere else

All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed on paper files.

Employers must be careful how they monitor e-mail

Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so. Monitoring the content of e-mail messages is a more sensitive matter and if you intend to do this you will need to be able to prove that you have the consent of staff. If you intend to monitor staff e-mail or telephone calls you should inform them how you intend to do this and who will carry out the monitoring.

The Information Commissioner's Employment Practices Code is an excellent guide to this subject.

E-mail is one of the most common causes of stress in the work-place

Whilst e-mail can be used to bully or harass people, it is more often the sheer volume of e-mail which causes individuals to feel that they have lost control of their e-mail and their workload. Regular filing and deletion can prevent this happening.

3. Creating and sending e-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail?

Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails.

When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.

Use a consistent method of defining a subject line

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

• Do not use text language or informal language in school e-mails.
• Always sign off with a name (and contact details).
• Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
• Never write a whole e-mail in capital letters. This can be interpreted as shouting.
• Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.
• If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list

can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

There is some debate about how enforceable disclaimers are. Legal advice should be sought when using or drafting a disclaimer for your organisation to ensure it meets your specific needs.

3. Creating and sending e-mail

Here are some steps to consider when sending e-mail.

Do I need to send this e-mail?

Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face.

To whom do I need to send this e-mail?

Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary. Never send on chain e-mails.

When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address.

Use a consistent method of defining a subject line

Having a clearly defined subject line helps the recipient to sort the e-mail on receipt. A clear subject line also assists in filing all e-mails relating to individual projects in one place. For example, the subject line might be the name of the policy, or the file reference number.

Ensure that the e-mail is clearly written

• Do not use text language or informal language in school e-mails.
• Always sign off with a name (and contact details).
• Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.
• Never write a whole e-mail in capital letters. This can be interpreted as shouting.
• Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.

• If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.

Sending attachments

Sending large attachments (e.g. graphics or presentations) to a sizeable circulation list can cause resource problems on your network. Where possible put the attachment in an appropriate area on a shared drive and send the link round to the members of staff who need to access it.

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

There is some debate about how enforceable disclaimers are. Legal advice should be sought when using or drafting a disclaimer for your organisation to ensure it meets your specific needs

4. Managing received e-mails

This section contains some hints and tips about how to manage incoming e-mails.

a) Manage interruptions

Incoming e-mail can be an irritating distraction. The following tips can help manage the interruptions.

• Turn off any alert that informs you e-mail has been received
• Plan times to check e-mail into the day (using an out of office message to tell senders when you will be looking at your e-mail can assist with this).

b) Use rules and alerts

• By using rules and alerts members of staff can manage their inbox into theme-based folders. For example:
• E-mails relating to a specific subject or project can be diverted to a named project folder
• E-mails from individuals can be diverted to a specific folder
• Warn senders that you will assume that if you are copied in to an e-mail, the message is for information only and requires no response from you.
• Internally, use a list of defined words to indicate in the subject line what is expected of recipients (for example:"For Action:", FYI:", etc)
• Use electronic calendars to invite people to meetings rather than sending e-mails asking them to attend

c) Using an out of office message

If you check your e-mail at stated periods during the day you can use an automated response to incoming e-mail which tells the recipient when they might expect a reply. A sample message might read as follows:
"Thank you for your e-mail. I will be checking my e-mail at three times today, 8:30am, 1:30pm and 3:30pm. If you require an immediate response to your e-mail please telephone me on 01964 542474."

This gives the sender the option to contact you by phone if they need an immediate response.

5. Filing e-mail

Attachments only

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

E-mail text and attachments

Where the text of the e-mail adds to the context or value of the attached documents it may be necessary to keep the whole e-mail. The best way to do this and retain information which makes up the audit trail, is to save the e-mail in .msg format. This can be done either by clicking and dragging the e-mail into the appropriate folder in an application such as MS Outlook, or by using the "save as" function to save the e-mail in an electronic filing system.

If the e-mail needs to be re-sent it will automatically open into MS Outlook.

Where appropriate the e-mail and the attachments can be printed out to be stored on a paper file, however, a printout does not capture all the audit information which storing the e-mail in .msg format will.

E-mail text only

If the text in the body of the e-mail requires filing, the same method can be used as that outlined above. This will retain information for audit trail purposes.

Alternatively the e-mail can be saved in .html or .txt format. This will save all the text in the e-mail and a limited amount of the audit information. The e-mail can not be re-sent if it is saved in this format.

The technical details about how to undertake all of these functions are available in application Help functions.

How long to keep e-mails?

E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards.

E-mail that needs to be kept should be identified by content; for example, does it form part of a pupil record? Is it part of a contract? The retention for keeping these e-mails will then correspond with the classes of records according to content in the retention schedule for schools found elsewhere in the Records Management Tool Kit for Schools.
These e-mails may need to be saved into any appropriate electronic filing system or printed out and placed on paper files.

APPENDIX 5

Safe disposal of records which have reached the end of their administrative life

NB: Please be aware that this guidance applies to all types of record, whether they are in paper or digital format.

1. Disposal of records that have reached the end of the minimum retention period allocated

The fifth data protection principle states that:

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

In each organisation, local records managers must ensure that records that are no longer required for business use are reviewed as soon as possible under the criteria set out so that only the appropriate records are destroyed.

The local review will determine whether records are to be selected for permanent preservation, destroyed, digitised to an electronic format or retained by the organisation for research or litigation purposes.

Whatever decisions are made they need to be documented as part of the records management policy within the organisation.

2. Safe destruction of records

All records containing personal information, or sensitive policy information should be made either unreadable or unreconstructable.
• Paper records should be shredded using a cross-cutting shredder
• CDs / DVDs / Floppy Disks should be cut into pieces
• Audio / Video Tapes and Fax Rolls should be dismantled and shredded
• Hard Disks should be dismantled and sanded

Any other records should be bundled up and disposed of to a waste paper merchant or disposed of in other appropriate ways. Do not put records in with the regular waste or a skip unless there is no other alternative.

There are companies who can provide confidential waste bins and other services which can be purchased to ensure that records are disposed of in an appropriate way.

1. Where an external provider is used it is recommended that all records must be shredded on-site in the presence of an employee. The organisation must also be able to prove that the records have been destroyed by the company who should provide a Certificate of Destruction. Staff working for the external provider should have been trained in the handling of confidential documents.

The shredding needs to be planned with specific dates and all records should be identified as to the date of destruction.

It is important to understand that if the records are recorded as to be destroyed but have not yet been destroyed and a request for the records has been received they MUST still be provided.

2. Where records are destroyed internally, the process must ensure that all records are recorded are authorised to be destroyed by a Senior Manager and the destruction recorded. Records should be shredded as soon as the record has been documented as being destroyed.

Freedom of Information Act 2000 (FoIA 2000)
The Freedom of Information Act 2000 requires the school to maintain a list of records which have been destroyed and who authorised their destruction10. Members of staff should record at least:
• File reference (or other unique identifier);
• File title (or brief description);
• Number of files and date range
• The name of the authorising officer
• Date action taken

Following this guidance will ensure that the school is compliant with the Data Protection Act 1998 and the Freedom of Information Act 2000.

3. Transfer of records to the Archives

Where records have been identified as being worthy of permanent preservation arrangements should be made to transfer the records to the County Archives Service. The school should contact the local record office if there is a requirement to permanently archive the records, and the records will continue to be managed via the DPA 1998 and the FoIA 2000.

If you would like to retain archive records in a special archive room in the school for use with pupils and parents please contact the local record office for specialist advice.

4. Transfer of information to other media

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as microform or digital media. The lifespan of the media and the ability to migrate data where necessary should always be considered.

Consideration should also be given to the legal admissibility of records that have been converted from paper to electronic media. It is essential to have procedures in place so that conversion is done in a standard way. This means that organisations can prove

that the electronic version is a genuine original and could not have been tampered with in any way. Reference should be made to 'British Standard 10008:2008 'Evidential weight and legal admissibility of electronic information' when preparing such procedures.

5. Recording of all archiving, permanent destruction and digitisation of records

Sample appendices are provided for the recording of all records to be used. These records could be kept in an Excel spreadsheet or other database format.

27. APPENDIX 6

Labels for retention to go on documents and files

All paper documents will need to include a retention sticker.

28. APPENDIX 7

Privacy notices – Parents

DATA PROTECTION ACT 2018

Privacy Notice (How we use pupil information)

• The categories of pupil information that we process include:
• personal identifiers and contacts (such as name, unique pupil number, contact details and address)
• characteristics (such as ethnicity, language, and free school meal eligibility)
• attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
• assessment and attainment (such as key stage 1 and phonics results, teacher assessments)
• medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
• safeguarding information (such as court orders and professional involvement)
• special educational needs (including the needs and ranking)
• behavioural information (such as exclusions and any relevant alternative provision put in place)
• Pupil Premium Eligibility (such as Looked After Status and Forces)
• information from other Agencies for the wellbeing safeguarding and protection of children.
• Further information provided by parents/carers.

Why we collect and use this information

We collect and use pupil information, for the following purposes:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections

The lawful basis on which we use this information

We collect and use pupil information as we have a legal obligation under the Education Act 1996 because we are providing a public service. Data processed is special category data from the GDPR-from 25 May 2018.
This information can be found in the census guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools
How we collect pupil information
We collect pupil information via registration forms at the start of the school year and via the Common Transfer File (CTF) or secure file transfer from previous schools

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data
We hold pupil data according the legal requirements set for each data category. These can be found on the in APPENDIX 2 our data protection policy, under Data Retention strategy. The Retention Schedule is divided into five sections:
1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Pupil Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

Who we share pupil information with
We routinely share pupil information with:

• schools that the pupil's attend after leaving us
• our local authority
• the Department for Education (DfE)

Why we share pupil information
We do not share information about our pupils with anyone without consent unless the law and our policies allow us to do so.
We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.
Department for Education
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under: section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.
All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

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.

Requesting access to your personal data
Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs. Anne Tennison : leven.sbm.primary@eastriding.gov.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
• a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to 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:
Mrs. Anne Tennison, Data Protector Officer
Leven.sbm.primary@eastriding.gov.uk

How Government uses your data
The pupil data that we lawfully share with the DfE through data collections:
• underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
• informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
• supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

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

The National Pupil Database (NPD)
Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).
The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to:
https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department
The law allows the Department to share pupils' personal data with certain third parties, including:
• schools
• local authorities
• researchers
• organisations connected with promoting the education or wellbeing of children in England
• other government departments and agencies
• organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.
For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

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

STAFF AND GOVERNORS
DATA PROTECTION ACT 2018
Privacy Notice (How we use school workforce information)

The categories of school workforce information that we collect, process, hold and share include:
• personal information (such as name, employee or teacher number, national insurance number)
• special categories of data including characteristics information such as gender, age, ethnic group, nationality, passport
• contract information (such as start dates, hours worked, post, roles and salary information)
• work absence information (such as number of absences and reasons)
• relevant medical information
• qualifications
• disclosure information, DBS, prohibited from teaching register, EEA Restrictions (Teachers who have lived/worked outside the UK.
• first aid training

• other training completed and inductions completed
• information regarding the right to work in the UK
• pecuniary interests
• references

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 employed and be paid
• safeguard pupils and vulnerable adults
• To meet statutory requirements re: the school's website e.g. Governor information

The lawful basis on which we use this information
We collect and use pupil information as we have a legal obligation under the Education Act 1996 because we are providing a public service. Data processed is special category data from the GDPR-from 25 May 2018.
This information can be found in the census guide documents on the following website https://www.gov.uk/education/data-collection-and-censuses-for-schools

Collecting this information
We collect personal information via, staff contract and application forms.

Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing this information
We hold Workforce data according the legal requirements set for each data category. These can be found on the in APPENDIX 2 the Data Retention strategy.

The Retention Schedule is divided into five sections:
1. Management of the School
2. Human Resources
3. Financial Management of the School
4. Property Management
5. Pupil Management
6. Curriculum Management
7. Extra-Curricular Activities
8. Central Government and Local Authority

Who we share this information with
We routinely share this information with:

• our local authority
• the Department for Education (DfE)

Why we share school workforce information
We do not share information about workforce members with anyone without consent unless legal responsibilities allow us to do so.

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

Department for Education (DfE)
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:

section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Requesting access to your personal data
Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Mrs. Anne Tennison, Data Protection Officer: leven.sbm.primary@eastriding.gov.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
• a right to seek redress, either through the ICO, or through the courts

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

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

Mrs. Anne Tennison, Data Protection Officer: leven.sbm.primary@eastriding.gov.uk

How Government uses your data
The workforce data that we lawfully share with the DfE through data collections:

• informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
• links to school funding and expenditure
• supports 'longer term' research and monitoring of educational policy

Data collection requirements
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.

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

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

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

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

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

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

APPENDIX 8

Letters to parents and staff

Dear Colleagues,

As you are aware, on 25th May 2018 there is a big change happening to privacy laws in the UK.

The new General Data Protection Regulation (GDPR) gives everyone more control over how personal information is used in all aspects of our lives and of course our children's lives.
As we've always done, we will continue to collect, use and store your data safely and securely.

What follows is a Privacy Statement.

You will have seen a similar one in the Prospectus. What follows is an updated version to comply with the new data protection regulations.
It explains:
• The categories of school workforce information that we collect, process, hold and share
• Why we collect and use this information
• The lawful basis on which we use this information
• Collecting and storing this information
• With who and why we share this information
• Requesting access to your personal data
• How Government uses your data

I hope you find it useful and reassuring. Further information can be found on the school website under the Policies Tab. Look for Data Protection.
http://levenprimary.eriding.net/home.aspx

Yours sincerely

Andrew Dolman
Head Teacher

(followed by privacy notice)

Dear Parents/Carers,

On 25th May 2018 there is a big change happening to privacy laws in the UK.

The new General Data Protection Regulation (GDPR) gives everyone more control over how personal information is used in all aspects of our lives and of course our children's lives.

As we've always done, we will continue to collect, use and store your data safely and securely.

What follows is a Privacy Statement.

You will have seen a similar one in the Prospectus. What follows is an updated version to comply with the new data protection regulations.
It explains:
• the data we hold
• why we collect and use this information
• the lawful basis on which we use this information
• how we store pupil data
• why we share pupil information
• your rights
• contact details
• and how the Government uses your data.

I hope you find it useful and reassuring. Further information can be found on the school website under the Policies Tab. Look for Data Protection.
http://levenprimary.eriding.net/home.aspx

Yours sincerely

Andrew Dolman
Head Teacher

(followed by privacy notice)