Elemore Hall School

Policy Title	**General Data Protection Regulation Policy**

This version	**November 2018**
Approved by	**FGB**
To be reviewed by	**Finance, Personnel and School Environment Committee**
Review Due	**November 2019**

Contents

1. Aims & Objectives

Elemore Hall School is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act 1998.

The school holds and processes information about employees, pupils, and other data subjects for academic and administrative purposes. When handling such information, the school, and all staff or others who process or use any personal information, must comply with the Data Protection Principles as outlined in the Act.

Changes to the data protection legislation which comes into effect from May 2018, (General Data Protection Regulations, GDPR) shall be monitored and implemented in order to remain compliant with all requirements.

The definitions of personal and sensitive data shall be as those published by the Information Commissioner's Office (ICO).

The principles of the Data Protection Act shall be applied to all data processed.

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data;
- how personal data should be processed, stored, archived and disposed of, and
- how staff, parents and pupils can access personal data.

1.1. It is a statutory requirement for all schools to have a Data Protection Policy:

(http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools)

1.2. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In Addition article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', is able to show that its policies and systems comply with requirements of GDPR.

2. Lawful Basis for Processing Data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that the school collects and processes is required to enable the performance of tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that the school is likely to rely on.

2.1 Age - Children under the age of 13 are not considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians do this on their behalf. Over the age of 13 this responsibility is transferred to the child and parents will not have responsibility for their child's data. (This is subject to the Data Protection Bill becoming law. The 'default' age under the GDPR is 16.)

2.2 Consent - If there is a lawful basis for collecting data then consent to collect data is not required. For example an employee could not opt to withhold an NI number. However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This is covered in more detail in section 5.2 and explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

2.3 Rights

The GDPR creates some new rights for individuals and strengthens some existing ones. It provides for the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Further detailed information on the rights can be found at Appendix 2.

For "privacy notices" covering the right to be informed, please see Appendix 3 and section 5 below.

Different rights attach to different lawful bases of processing:

	Right to Erasure	Right to Portability	Right to Object
Vital Interests	✓	X	X
Legal Obligation	X	X	X
Public Task	X	X	✓
Legitimate Interests	✓	X	✓
Contract	✓	✓	X
Consent	✓	✓	But right to withdraw consent

The right to erasure - GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. It will be seen from the table above that where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above) there is no right to erasure – however this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

3. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff is used to managing risk, ensuring it is assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach" which could result in legal action against the school. The loss of sensitive, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

3.1. Personal Data

The school has access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances.

- Personal information about members of the school community – including pupils, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records.
- Curricular / academic data e.g. class lists, pupil progress records, reports, references.
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references.
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

3.2. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff;
- information about the sexuality of a child, his or her family or a member of staff;
- medical information about a child or member of staff (SEND); and
- some information regarding safeguarding will also fall into this category. Staffing e.g. Staff Trade Union details.

3.3 Other Types of Data Not Covered by the Act

This is data that does not identify a living individual and therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include lesson plans (where no individual pupil is named), teaching resources and other information about the school which does not relate to an individual.

Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

The ICO provides additional information on their website.
See http://ico.org.uk/for_organisations/data_protection/the_guide/key_definitions

4. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection; The Headteacher is the Data Controller, Data Protection Officer to manage data on a day to day basis is Hilary Johnson-Browne, Head of Support Services. The Network Manager, Ian Clifton has responsibility for ICT within the school and ITSS manage the administration network ie SIMS and FMS.

4.1. Risk Management – Roles: Data Protection Officer

The school should have a nominated member of staff responsible for the management of data protection.

According to the ICO the minimum role will include:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws;
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

4.2. Risk management - Staff and Governors Responsibilities

- Everyone in the school has the responsibility of handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

5. Legal Requirements

5.1. Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration:

http://ico.org.uk/for_organisations/data_protection/registration

5.2. Information for Data Subjects (Parents, Staff): Privacy Notices

Elemore Hall School shall be transparent in relation to intended processing of data and communicate these intentions through notification to staff, parents and pupils prior to the processing of individual's data. Communication shall be in the form of an information notice and letter which has been sent to parents prior to the new regulations coming into place on 25 May 2018 and will be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-noticestransparency-and-control/

There may be circumstances where the school is required either by law or in the best interests of our pupils or staff to pass information onto external authorities, for example Local Authorities, Ofsted, or the Department of Health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them. Under no circumstances will the school disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition;
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child;
- recorded by the pupil in an examination;
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed, and
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

In order to comply with the fair processing requirements of the DPA, the school **will** inform parents / carers of all pupils / students and staff of the data they collect, process and hold on the pupils / students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. This privacy notice will be passed to parents / carers through an information notice and letter.

http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

New privacy notices will be issued to all 'data subjects' by May 2018 even if the data subject has previously received a similar notice. This is because of the new rights in the GDPR that people should be informed about.

6. Transporting, Storing and Disposing of Personal Data

6.1. Information Security - Storage and Access to Data

Access to computers are all password protected. These are set by the Network Manager on a termly basis. Those systems that hold more sensitive/identifiable information have extra layers of security.

The data is stored on servers which are held in a secure room which only the Network Manager, Headteacher and Head of Support Services have access to.

6.1.1. Technical Requirements

- The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for three minutes if no keystrokes are detected.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. We are aware of and understand the higher risk of a data loss and the possibility of a cyber attack and have appropriate measures in place to deal with such an event. See Appendix 3

6.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected;
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected);
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete;
- the school has set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices; and
- only encrypted removable storage purchased by the school is allowed to be used on school computers.

6.1.3. Passwords

- All users will use strong passwords which must be changed regularly. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

6.1.4. Images

- The school records and stores images in accordance with our privacy and photo/video agreements. Permission for this will be obtained in the privacy notice or other photographic permission notice provided to parents / carers.
- Images will be protected and stored in a secure area.

6.1.5. Cloud Based Storage

The school has a clear policy and procedures for the use of "Cloud Based Storage Systems". These are included within the Online Policy. The school and its personnel are aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school is satisfied with controls put in place by remote / cloud based data services providers to protect the data. See advice from the DfE below:-

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

6.2. Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party as well as data processing agreements.

http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

6.3. Retention of Data

- The guidance given by the Information and Records Management Society – Schools records management toolkit will be used to determine how long data is retained.
- Personal data that is no longer required will be destroyed and this process will be recorded.

6.4. Systems to Protect Data

6.4.1. Paper Based Systems

- All paper based personal data will be protected by appropriate controls, for example:

  - paper based safeguarding chronologies will be in a locked cupboard when not in use; and
  - class lists used for the purpose of marking may be stored in a teacher's bag.

6.4.2. School Websites

- Uploads to the school website will be checked prior to publication, for instance:

  - to check that appropriate photographic consent has been obtained; and
  - to check that the correct documents have been uploaded.

Only the Headteacher and the Network Manager have the appropriate level of access to upload and amend the content of the website. Any queries or requests must in all instances be forwarded to them for approval and uploading.

6.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

- Where technically possible all email containing sensitive information will be encrypted by this may be carried out by attaching the sensitive information as a word document and encrypting the document / compressing with 7 zip and encrypting. The recipient will then need to contact the school for access to a one-off password), or
- The use of Egress (Secure email system) allows for secure communication.

7 Data Sharing

The school is required by law to share information with the LA and DfE. Further details are available at:
https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Durham LSCB also provides information on information sharing at:

http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

Schools should ensure that, where special category data is shared, it is transmitted securely for instance by secure email such as Egress or is delivered to the named recipient by hand.

8 Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records; it can also mean inappropriate access to information.

- In the event of a data breach the Data Protection Officer will inform the Headteacher and Chair of Governors.
- The school will follow the procedures set out in Appendix 6.

9 Policy Review

This policy will be reviewed and updated if necessary every two years or when there are relevant legislative changes.

Date: _____ Review: _____

Signed:
Chair of Governors

Adopted by the Governing Body on _____

The Data Protection Officer is _____

Appendix 1

ICO Guidance on GDPR
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr

http://ico.org.uk/for_organisations/sector_guides/education

Specific information for schools is available here. This includes links to guides from the DfE

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv
Specific Information about CCTV

Information and Records Management Society – Schools records management toolkit

http://irms.org.uk/page/SchoolsToolkit
A downloadable schedule for all records management in schools

Disclosure and Barring Service (DBS)

https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information
Details of storage and access to DBS certificate information.

DFE Privacy Notices

https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

DFE Use of Biometric Data

https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Appendix 2

The right to be informed

The privacy notice supplied to parents/carers, pupils and staff in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. If services are offered directly to a pupil, the school will ensure that the privacy notice is written in a clear, plain manner that the pupil will understand. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The name and contact details of the Data Controller and where applicable, the controller's representative and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the Data Controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third parties and the safeguards in place.
- The retention period and criteria used to determine the retention period.

The existence of the data subject's rights, including the right to:

- Withdraw consent at any time
- Lodge a complaint with a supervisory authority.

The existence of automated decision making including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

The right of access

Individuals have the right to obtain confirmation that their data is being processed.
Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified.
Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the individual withdraws their consent;
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data is required to be erased in order to comply with a legal obligation; and
- The personal data is processed in relation to the offer of information society services to a child.

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; and
- The exercise or defence of legal claims.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing

Individuals have the right to block or suppress the school's processing of personal data.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data;
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual;
- Where processing is unlawful and the individual opposes erasure and requests restriction instead; and
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school will inform individuals when a restriction on processing has been lifted.

The right to data portability

Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract; and
- When processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form.

The school will provide the information free of charge.

Where feasible, data will be transmitted directly to another organisation at the request of the individual.

Elemore Hall School is not required to adopt or maintain processing systems which are technically compatible with other organisations.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest;
- Direct marketing; and
- Processing for purposes of scientific or historical research and statistics.
-

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation; and
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received; and
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object; and
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

Appendix 3

Privacy notice for parents/carers

Elemore Hall School

Privacy notice for parents/carers

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about **pupils**.

We, Elemore Hall School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Hilary Johnson Browne (see 'Contact us' below).

Who we are and what we do

We are Elemore Hall School, Pittington, Durham, DH6 1QD. We are a maintained Special school for Secondary aged pupils who have SEMH. Our local authority is Durham County Council.

The personal data we hold

We hold personal data about pupils, their parents or carers to support teaching and learning, to provide pastoral care, to facilitate safeguarding and support for the pupil in the wider wolrd and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities, health care providers and the Department of Education. Personal data that we may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:

- Contact details, contact preferences, date of birth, identification documents, unique pupil number, unique candidate number
- Results of internal assessments and externally set tests
- Academic and personal & social skills assessment information and records
- Pupil and curricular records/reports
- Records of Home and Other Agency contact and meetings
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Positive and Negative behaviour records
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Medical and Social Care records (where relevant)
- EHCP and review documentation
- Details of any support received, including care packages, plans and support providers
- Photographs
- CCTV images captured in school

We may also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services
- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing

Our legal basis for using this data

You may wish to refer to the ICO's guidance on the lawful basis for processing.

We only collect and use pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process pupils' personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual's vital interests (or someone else's interests)

Where we have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using pupils' personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

While the majority of information we collect about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you or your child, we make it clear whether providing it is mandatory or optional. If it is mandatory, we will explain the possible consequences of not complying.

We collect/obtain data from pupils, parents, carers, teachers, other professionals (eg. GP, Hospital, Social Workers, etc), public bodies (Department of Education, Durham County Council) and those organisations with tied links to the DofE, for example Fisher Family Trust.

How we store this data

We keep personal information about pupils while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. Our Records Management Policy sets out how long we keep information about pupils.

The security of data and information is important to us. This ius why we follow a range of security policies and procedures to control and safeguard access to and use of your personal information – this includes both physical and technical security and integrity of all data.

Our Records Management Policy is available on the school website - www.elemorehallschool.com

For more information you may wish to refer to the Information and Records Management Society's toolkit for schools

Data sharing

We do not share any data about you or your child with any third party without your permission unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about pupils with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and exclusions;
- The Department for Education (and the Education Funding Agency) – to meet our legal obligations to share certain information with it, such as attendance, exclusions and KS4 results;
- The pupil's family and representatives – to ensure that they are fully informed in their capacity as parents/legal guardians;
- Educators and examining bodies – to ensure that there is sufficient, accurate information to allow for accurate record keeping and entry for public examinations to take place;
- Our regulator Ofsted and Ofsted (NMS) – to meet our obligations under the inspection frameworks;
- Suppliers and service providers – to enable them to provide the service we have contracted them for;
- Central and local government – to enable them to support, fund and audit the school appropriately;
- Our auditors – to ensure that the school operates lawfully;
- Health authorities – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Security organisations – to meet our lawful duty;
- Health and social welfare organisations – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Professional advisers and consultants – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Charities and voluntary organisations – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Police forces, courts, tribunals – to comply with our lawful duty;
- Professional bodies – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP.

National Pupil Database

We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

Youth support services

Once our pupils reach the age of 13, we are legally required to pass on certain information about them to the Improving Progression Team in CYPS Durham County Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Parents/carers, or pupils once aged 16 or over, can contact our data protection officer to request that we only pass the individual's name, address and date of birth to the Improving Progression Team in CYPS Durham County Council.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

Parents/carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 16), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, and if we do hold information about you or your child, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request please contact our data protection officer.

Parents/carers also have a legal right to access to their child's **educational record**. To request access, please contact Michael Hunter (Deputy Headteacher). The school will respond within 15 days.

If we cannot provide information to you, we will give you a description of the information we hold and the reason why it cannot be disclosed to you at the time of your request.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

- Hilary Johnson-Browne

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way we use data in this school.

Elemore Hall School

Privacy notice for pupils

Privacy notice for pupils

You have a legal right to be informed about how our school uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data.

This privacy notice explains how we collect, store and use personal data about you.

We, Elemore Hall School, Pittington, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Hilary Johnson-Browne (see 'Contact us' below).

The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

This information includes:

- Your contact details
- Your assessment results
- Your attendance records
- Your characteristics, like your ethnic background or any special educational needs
- Your Education, Health & Care Plan (EHCP)
- Your educational records
- Any medical conditions you have
- Details of any behaviour issues or exclusions
- Photographs
- CCTV images

Why we use this data

We use this data to help run the school, including to:

- Get in touch with you and your parents when we need to
- Check how you're doing in subjects and assessments and work out whether you or your teachers need any extra help
- Provide you with the best possible experiences to support your personal, social and academic development
- Track how well the school as a whole is performing
- Look after your wellbeing
- Keep people safe

- Identify areas where the school can improve how it works

Our legal basis for using this data

We will only collect and use your information when the law allows us to. Most often, we will use your information where:

- We need to comply with the law
- We need to use it to carry out a task in the public interest (in order to provide you with an education)

Sometimes, we may also use your personal information where:

- You, or your parents/carers have given us permission to use it in a certain way
- We need to protect your interests (or someone else's interest)

Where we have got permission to use your data, you or your parents/carers may withdraw this at any time. We will make this clear when we ask for permission, and explain how to go about withdrawing consent.

Some of the reasons listed above for collecting and using your information overlap, and there may be several grounds which mean we can use your data.

Collecting this information

We collect data from a wide range of sources but mainly from yourself, your parents/carers, your educational records and school staff, health and social care professionals and information that is provided to us by local and national government departments.

While in most cases you, or your parents/carers, must provide the personal information we need to collect, there are some occasions when you can choose whether or not to provide the data.

We will always tell you if it's optional. If you must provide the data, we will explain what might happen if you don't.

How we store this data

We will keep personal information about you while you are a pupil at our school. We may also keep it after you have left the school, where we are required to by law.

We have a Records Management Policy which sets out how long we must keep information about pupils.

The Records Management Policy is on the website but you can also ask for a copy from Hilary Johnson-Browne.

Data sharing

We do not share personal information about you with anyone outside the school without permission from you or your parents/carers, unless the law and our policies allow us to do so.

Where it is legally required, or necessary for another reason allowed under data protection law, we may share personal information about you with:

- The Department for Education – to meet our legal obligations to share certain information with it, such as attendance, exclusions and KS4 results;
- Your family and representatives – to ensure that they are fully informed in their capacity as parents/legal guardians;
- Educators and examining bodies – to ensure that there is sufficient, accurate information to allow for accurate record keeping and entry for public examinations to take place;
- Our regulator Ofsted and Ofsted (NMS) – to meet our obligations under the inspection frameworks;
- Suppliers and service providers – to enable them to provide the service we have contracted them for;
- Central and local government – to enable them to support, fund and audit the school appropriately;

- Our auditors – to ensure that the school operates lawfully;
- Health authorities – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Security organisations – to meet our lawful duty;
- Health and social welfare organisations – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Professional advisers and consultants – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Charities and voluntary organisations – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Police forces, courts, tribunals – to comply with our lawful duty;
- Professional bodies – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP.

National Pupil Database

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database, which is managed by the Department for Education and provides evidence on how schools are performing. This, in turn, supports research.

The database is held electronically so it can easily be turned into statistics. The information it holds is collected securely from schools, local authorities, exam boards and others.

The Department for Education may share information from the database with other organisations which promote children's education or wellbeing in England. These organisations must agree to strict terms and conditions about how they will use your data.

You can find more information about this on the Department for Education's webpage on how it collects and shares research data.

You can also contact the Department for Education if you have any questions about the database.

Youth support services

Once you reach the age of 13, we are legally required to pass on certain information about you to the Improving Progression Team, CYPS, Durham County Council, as it has legal responsibilities regarding the education or training of 13-19 year-olds.

This information enables it to provide youth support services, post-16 education and training services, and careers advisers.

Your parents/carers, or you once you're 16, can contact our data protection officer to ask us to only pass your name, address and date of birth to the Improving Progression Team, CYPS, Durham County Council.

Transferring data internationally

Where we share data with an organisation that is based outside the European Economic Area, we will protect your data by following data protection law.

Your rights

How to access personal information we hold about you

You can find out if we hold any personal information about you, and how we use it, by making a **'subject access request'**, as long as we judge that you can properly understand your rights and what they mean.

If we do hold information about you, we will:

- Give you a description of it

- Tell you why we are holding and using it, and how long we will keep it for
- Explain where we got it from, if not from you or your parents
- Tell you who it has been, or will be, shared with
- Let you know if we are using your data to make any automated decisions (decisions being taken by a computer or machine, rather than by a person)
- Give you a copy of the information

You may also ask us to send your personal information to another organisation electronically in certain circumstances.

If you want to make a request please contact our data protection officer.

Your other rights over your data

You have other rights over how your personal data is used and kept safe, including the right to:

- Say that you don't want it to be used if this would cause, or is causing, harm or distress
- Stop it being used to send you marketing materials
- Say that you don't want it used to make automated decisions (decisions made by a computer or machine, rather than by a person)
- Have it corrected, deleted or destroyed if it is wrong, or restrict our use of it
- Claim compensation if the data protection rules are broken and this harms you in some way

Complaints

We take any complaints about how we collect and use your personal data very seriously, so please let us know if you think we've done something wrong.

You can make a complaint at any time by contacting our data protection officer.

You can also complain to the Information Commissioner's Office in one of the following ways:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer:

- Hilary Johnson-Browne, Head of Support Services, Elemore Hall School

This notice is based on the Department for Education's model privacy notice for pupils, amended to reflect the way we use data in this school.

Elemore Hall School

Privacy notice for staff

Privacy notice for staff

Under data protection law, individuals have a right to be informed about how the school uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage, to work at our school.

We, Elemore Hall School, Pittington, Durham, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Hilary Johnson-Browne (see 'Contact us' below).

The personal data we hold

You may find it helpful to refer to the ICO's definitions of 'personal data' and 'special categories of personal data' based on the General Data Protection Regulation.

We process data relating to those we employ, or otherwise engage, to work at our school. Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in an application form, CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information and professional development records
- Outcomes of any disciplinary and/or grievance procedures
- Absence data – including LoA and Sickness
- Copy of driving licence
- Personal vehicle details
- Photographs/Videos
- CCTV footage
- Data about your use of the school's information and communications system

We may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why we use this data

The purpose of processing this data is to help us run the school, including to:

- Support you in your professional role
- Monitor and report on school improvement and self-evaluation
- Provide appropriate pastoral care
- Protect pupil welfare
- Ensure that the information we hold about you is kept up to date
- Share with agencies such as payroll and pensions
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body or other relevant review body
- To maintain security

Our lawful basis for using this data

You may wish to refer to the ICO's guidance on the lawful basis for processing.

We only collect and use personal information about you when the law allows us to. Most commonly, we use it where we need to:

- Fulfil a contract we have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, we may also use personal information about you where:

- You have given us consent to use it in a certain way
- We need to protect your vital interests (or someone else's interests)

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the school's use of your data.

Collecting this information

While the majority of information we collect from you is mandatory, there is some information that you can choose whether or not to provide to us.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

How we store this data

We keep personal information about staff while they are working at our school. We may also keep it beyond their time at our school if this is necessary in order to comply with our legal obligations.

We will only retain the data we collect for as long as is necessary. This would be to satisfy the purpose for which it has been collected in accordance with our Records Management Policy, this can be found on the internal network under “Staff Share” - “Policies”

The security of data and information is important to us. This is why we follow a range of security policies and procedures to control and safeguard access to and use of your personal information. This includes both physical and technical security and integrity of all data.

Examples of our security include:

- Encryption, meaning that information is hidden so that it cannot be read without access knowledge (such as a password). This is done with a secret code or what’s called a ‘cypher’. The hidden information is said to then be ‘encrypted’;
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it;
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong;
- Regular testing of our technology and ways of working including keeping up to date on the latest security updates (commonly called patches);

Data sharing

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law) we may share personal information about you with:

- Our local authority – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about headteacher performance and staff dismissals;
- The Department for Education - to meet our legal obligations to share certain information with it;
- Examining or Awarding bodies – if you are the relevant member of staff to enable them to provide the service we have contracted them for;
- Our regulator (Ofsted and Ofsted (NMS) – to meet our obligations under the inspection frameworks;
- Suppliers and service providers – to enable them to provide the service we have contracted them for, such as payroll;
- Employment and recruitment agencies – when seeking or providing a reference (only with your permission)

- Central and local government – to enable them to support, fund and audit the school appropriately;
- Our auditors – to ensure that the school operates lawfully;
- Health authorities – to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Security organisations – to meet our lawful duty;
- Health and social welfare organisations – where appropriate/relevant to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Professional advisers and consultants – where appropriate/relevant to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Charities and voluntary organisations – where appropriate/relevant to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- Police forces, courts, tribunals – to comply with our lawful duty;
- Professional bodies – where appropriate/relevant to ensure that they have crucial information to enable the best service for pupils and their families as agreed within the EHCP;
- HMRC
- DBS
- Pension schemes.

If you would like confirmation of who we do share information with please contact us.

At no time will your information be passed to organisations external to us for marketing or sales purposes or for any other commercial use without your prior consent.

Transferring data internationally

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

Your rights

How to access personal information we hold about you

Individuals have a right to make a **'subject access request'** to gain access to personal information that the school holds about them.

If you make a subject access request, and if we do hold information about you, we will:

- Give you a description of it
- Tell you why we are holding and processing it, and how long we will keep it for
- Explain where we got it from, if not from you
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact our data protection officer.

Your other rights regarding your data

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:

- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our **data protection officer**:

- HilaryJohnson-Browne

This notice is based on the Department for Education's model privacy notice for the school workforce, amended to reflect the way we use data in this school.

Appendix 4

GDPR - The General Data Protection Regulation.

These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR

All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:

The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR. The ICO website is http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:

General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:

General information note from the Information Commissioner on publication of examination results.

Education Act 1996:

Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:

Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:

Retention requirements for a range of Health and Safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:

Retention of school admission and exclusion appeal papers and other pupil records.

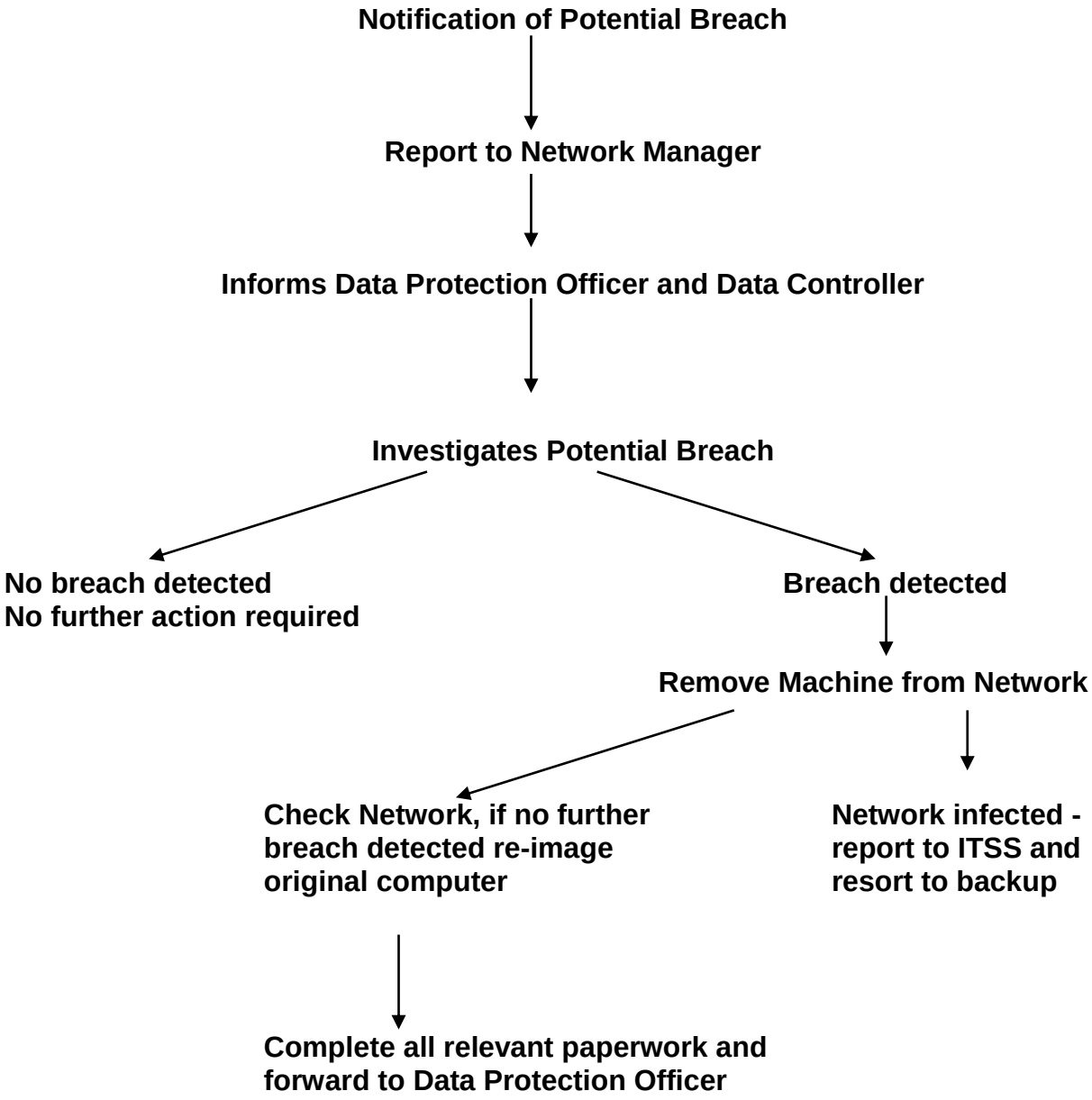
Appendix 5

Schools may find it beneficial to use this to check their systems for handling data.

- Data Protection Officer in place
- Information asset log complete
- School able to demonstrate compliance with GDPR
- Training for staff on Data Protection, and how to comply with requirements
- Data Protection Policy in place
- All portable devices containing personal data are encrypted
- Passwords – Staff use complex passwords
- Passwords – Not shared between staff
- Privacy notice sent to parents/pupils aged 13 or over
- Privacy notice given to staff
- Images stored securely
- School registered with the ICO as a data controller
- Systems in place to ensure that data is retained securely for the required amount of time
- Process in place to allow for subject access requests
- If school has CCTV, appropriate policies are in place to cover use, storage and deletion of the data, and appropriate signage is displayed
- Paper based documents secure
- Electronic backup of data both working and secure
- Systems in place to help reduce the risk of a data breach *e.g. personal data sent out checked before the envelope sealed, uploads to websites checked etc*

Appendix 6

POTENTIAL DATA BREACH FLOWCHART



Appendix 7

School census and workforce census

The school census is a statutory return completed by all state sector schools and academies within England. Data is collected on the third Thursday in January and May and the first Thursday in October. The School Workforce census takes place annually during the autumn term. Data items collected vary according to each census however; all returns include child and staffing level personal data. The school will provide Durham County Council and the DfE with the final versions of all census returns in a timely and appropriately secure manner via the SIMS system.

Categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility);
- Medical information (such as name of GP, relevant medical conditions);
- Attendance information (such as sessions attended, number of absence, absence reasons);
- Behavioural information (such as behaviour incidents, exclusions);
- Assessment information (such as national curriculum assessments);
- Special educational needs information (such as an Educational Health Care Plan EHCP);
- School history (such as where pupils go when they leave us.

Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in whether you wish to provide or not.

CCTV

The school has a CCTV system installed throughout the premises. The purpose of the system is help to provide a safe and secure environment for pupils, staff, visitors and contractors to the site. It also used for the purpose of preventing damage and loss to the fabric of the building and loss of property.

The school understands that recording images of identifiable individuals constitutes as processing personal information therefore, it is carried out in line with data protection principles. The school notifies all pupils, staff, visitors, Governors and contractors to the site of the purpose of collecting CCTV images via information points, code of conduct policy and privacy notices.

Cameras are only positioned where they do not intrude upon anyone's privacy and are there to fulfil the purpose of security in and around the buildings. The Data Processer Officer is responsible for the management, storage, security and retention of any CCTV footage. There is a limited amount of staff who use the system and who are responsible for providing information, when appropriate to do so, to other authorities such as the

Police. Any information leaving the site will be on encrypted CD or USB which is signed for by the receiving Officer. Retention of material is kept in accordance with the records management policy.

Texting Services

The school uses a texting service, Teachers 2 Parents (T2P) to contact parents/carers and staff of relevant details regarding the school, for example school closures, pupil attendance etc. If anyone does not wish to be part of this service and has the intention to withdraw they must in the first instance contact to discuss this request.

Complaints

Complaints and queries received by the school in relation to any aspect of the data protection collection, storage, security etc will be dealt with in line with the schools Complaints Policy which can be found on the school website or by contacting the school direct.

Further Information

If you require any further information that is not included in the above policy please contact the school on 0191 3720275 and ask for the Headteacher, Mr Richard Royle or the Head of Support Services, Mrs Hilary Johnson-Browne.

Subject Access Request (SAR)

Any request for data must be made in writing; which can include email. This must be addressed to the Data Protection Officer. It must clearly state in the correspondence the nature of the information required, if it is not then further inquiries will need to be undertaken to ascertain the precise nature of the request. Prior to any information being shared the following evidence of identity will need to be produced, this includes:

- Passport;
- Driving licence;
- Birth/marriage certificate;
- P45/60;
- Utility bills, within three months of date and must include present address; and/or
- Credit card or mortgage statement, within a three month date period.

Upon receipt of a SAR the response time is 15 school days, if the request relates to an educational record. For any other type of request then the response time is 40 calendar days, which includes holiday periods. This timeframe will commence after the receipt of any monies due for copying costs etc and if further clarification is needed regarding the information requested.

Charges

There may be charges incurred for the provision of information which can be dependent on the following:

- Should the information requested contain the educational record then the amount charged will be reliant upon the number of pages involved.
- If the information that is requested is of a personal nature and does not include any educational records then the school may make a charge of £10 to provide such information.
- If the information requested is only for the provision of the educational record viewing will be free of charge however, a cost for the copying of the information may be made, this decision will be made by the Headteacher.