Thomson House School

Data Protection & Freedom of Information Policy

Agreed by: Full Governing Board

Date: March 2023

Review Cycle: Every year

Review Date: March 2024

All the Thomson House School policies should be read in conjunction with the Equality Policy.

IF YOU REQUIRE A COPY OF THIS DOCUMENT IN LARGE PRINT, BRAILLE OR AUDIO FORMAT, PLEASE CONTACT THE HEAD OF FINANCE & OPERATIONS

1 POLICY STATEMENT

1.1 Thomson House School ('the School', 'we', 'us' and 'our') is committed to upholding individuals' rights to have their Personal Data protected. This policy is designed to meet the requirements of the General Data Protection Regulation. The school is registered with the ICO / has paid its data protection fee to the ICO, as legally required.

1.2 While carrying out its functions, the School will collect, store and process Personal Data about students, parents, employees and other third parties. Proper treatment of these data is essential and in line with the School's values.

1.3 All school staff are obliged to comply with this Policy when processing Personal Data on our behalf. Any breach of this Policy by School staff may result in disciplinary or other action.

2 ABOUT THIS POLICY

2.1 The School holds Personal Data about current, past and prospective students, parents, employees and others with whom the School communicates. As such the school is a Data Controller. Personal data may be recorded on paper or stored electronically.

2.2 This Policy and other documents referred to in it set out the basis on which the School will process any Personal Data it collects from individuals, whether those data are provided to us by individuals or obtained from other sources. It sets out the rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store Personal Data.

2.3 This Policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 The Data Protection Officer (DPO) is responsible for ensuring compliance with the Relevant Data Protection Laws and with this Policy. That post is held by the Head of Finance & Operations, 0203 608 2080, admin@thomsonhouseschool.org. Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

3 DEFINITION OF DATA PROTECTION TERMS

3.1 In this Policy, the functions of the School are the provision of education and any pastoral, business, administrative, community or similar activities associated with that provision. References to the School 'carrying out its functions' or similar are references to these activities.

3.2 References to 'we' are references to the School.

3.3 **Criminal Convictions and Offences** means the commission of, or proceedings for, any offence committed or alleged to have been committee by a person, the disposal of such proceedings or the sentence of any court in such proceedings.

3.4 **Data Subjects** means identified or identifiable natural persons whose Personal Data the School holds. This Policy also refers to Data Subjects as 'individuals.'

3.5 **Data Controllers** are the people who, or organisations which, determine the purposes for which any Personal Data are processed, including the means of the processing. The School is the Data Controller of all Personal Data used for carrying out its

functions. The Head Teacher acts as the representative of the data controller on a day-to-day basis

3.6 **Data Users** are, for the purposes of this Policy, those of our employees whose work involves processing Personal Data. Data Users must protect the data they handle in accordance with this Policy and any applicable data security procedures at all times. This Policy also refers to Data Users as 'School staff' or simply 'staff'.

3.7 **Data Processors** include any person or organisation, who is not a member of School staff, which processes Personal Data on our behalf. Employees of Data Controllers are excluded from this definition but it could include suppliers that handle Personal Data on the School's behalf.

3.8 **Fair Processing Notices** are documents explaining to Data Subjects how their data will be used by the School.

3.9 **Personal Data** means any information relating to an identified or identifiable natural person; 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 physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

3.10 **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 transmitted, stored or otherwise processed.

3.11 **Pseudonymisation** means the processing of Personal Data so that it can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

3.12 **Relevant Data Protection Law** means the General Data Protection Regulation including; Data Protection Act 2018 (DPA 2018), The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020, and all applicable laws and regulations relating to the processing of Personal Data and privacy as amended, re-enacted, replaced or superseded from time to time and where applicable the guidance and codes of practice issued by the United Kingdom's Information Commissioner.

3.13 The policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3.14 The policy also meets the requirement of The Freedom of Information Act 2000.

3.15 **Special Categories of Personal Data** (formerly known as 'sensitive Personal Data') include information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life and genetic or biological traits. Special Categories of Personal Data can only be processed under strict conditions.

4 DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data for or on behalf of the School must comply with the

principles of good practice contained in Relevant Data Protection Law. These principles state that Personal Data must be:

4.1.1 Processed lawfully, fairly and in a transparent manner;

4.1.2 Collected for specified, explicit and legitimate purposes;

4.1.3 Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;

4.1.4 Accurate and, where necessary, kept up to date;

4.1.5 Kept for no longer than is necessary for the purposes for which it is processed; or

4.1.6 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.

The School will keep a record of all data processing activities and must be able to demonstrate its compliance with these principles and with the wider requirements of Relevant Data Protection Law.

5 FAIR, LAWFUL AND TRANSPARENT PROCESSING

5.1 For Personal Data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in Relevant Data Protection Law. These include, but are not limited to:

5.1.1 the individual's explicit consent to the processing for one or more specified purposes;

5.1.2 that the processing is necessary for the performance of a contract with the individual or for the compliance with a legal obligation to which the School is subject;

5.1.3 The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent;

5.1.4 The data needs to be processed so that the school can comply with a legal obligation;

5.1.5 that the processing is in the public interest; or

5.1.6 that the processing is in the legitimate interest of the School or relevant third parties to which the data are disclosed, so long as this is balanced with the rights and freedoms of the individual.

5.1.7 Where a type of Data Processing is likely to pose a high risk to individuals' rights and freedoms, [for example when using closed-circuit television on the school site,] the School will carry out an appropriate Privacy Impact Assessment.

5.2 *Special Categories of Personal Data*

5.3 When Special Categories of Personal Data are being processed, the individual's explicit consent to processing of those data must be obtained unless the processing:

5.3.1 is necessary for the purposes of carrying out the obligations and exercising specific rights of the School or of the individual in the field of employment and social security and social protection law;

5.3.2 is necessary for the assessment of the working capacity of an individual where the individual is an employee or for the provision of health or social care;

5.3.3 relates to Personal Data which are manifestly made public by the individual;

5.3.4 The data needs to be processed for the establishment, exercise or defence of legal claims;

5.3.5 is necessary for reasons of substantial public interest; or

5.3.6 is necessary to protect the vital interests of the individual.

5.4 Processing of data relating to Criminal Convictions and Offences can only take place under control of an official authority, such as instructions from the police or an order of the court, or where UK or EU law states that processing must take place.

5.5 *Consent of adults and organisations*

5.6 Where an individual gives consent to Data Processing, that consent must be freely given, specific, informed and unambiguous and should be either in the form of a statement (whether or not prepared by the School) or a positive action demonstrating consent. Any requests that the School makes for consent must be in clear language.

5.7 An individual has the right to withdraw consent at any time and will be informed of this right and how to exercise it when the School requests consent.

5.8 *Consent of children and young people*

5.9 Parental consent to Data Processing must be obtained for pupils or other children younger than 13 years of age.

5.10 A young person aged 13 or over is, except where there are issues over mental capacity, able to give valid consent. Where a pupil reaches his or her 13th birthday while a pupil of an academy within the School, his or her consent should be obtained with reference to the requirements of 5.5 above.

6 PROCESSING FOR SPECIFIED, LIMITED AND LEGITIMATE PURPOSES

6.1 In the course of carrying out its functions, the School may collect and process the Personal Data set out in the Schedule. This may include data we receive directly from a an individual (for example, by completing forms or by corresponding with us by post, phone, email or otherwise) and data we receive from other sources (including, for example, the local authority or other public bodies, business suppliers or service providers, professional advisers and others).

6.2 The School will only process Personal Data for the specific purposes set out in the Schedule or for any other purposes specifically permitted by Relevant Data Protection Law. We will explain those purposes to the Data Subject.

7 ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

7.1 We will only collect Personal Data to the extent that it is required for the specific purpose notified to the individual;

7.2 If a member of staff has any doubt as to whether any processing exceeds the purposes for which that data were originally collected, he or she should notify the Data Protection Officer.

8 ACCURATE AND UP-TO-DATE DATA

8.1 We will ensure that Personal Data we hold are accurate and kept up to date. We will check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8.2 It is the responsibility of staff to ensure that Personal Data is accurate and kept up to date. Further, parents and anyone who provides Personal Data should also inform the School as soon as possible if there is any change to their Personal Data.

9 TIMELY PROCESSING

9.1 We will not keep Personal Data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which are no longer required. We will be guided by the Information Records Management Society guidance in respect of decision making concerning the retention of Personal Data.

9.2 If a member of staff has any doubt as to whether any Personal Data has been or will be kept longer than is necessary for the purpose or purposes for which they were collected, he or she should notify the Data Protection Officer.

10 PROCESSING SECURELY AND IN LINE WITH RIGHTS OF DATA SUBJECTS

10.1 We are committed to upholding the rights of individuals to access Personal Data the School holds on them.

10.2 We will process all Personal Data in line with individuals' rights, in particular their rights to:

10.2.1 be informed, in a manner which is concise, transparent, intelligible and easily accessible and written in clear and plain language, of the purpose, use, recipients and other processing issues relating to data;

10.2.2 receive confirmation as to whether your Personal Data is being processed by us;

10.2.3 access your Personal Data which we are processing only by formal written request. We may charge you for exercising this right if we are allowed to do so by Relevant Data Protection Law. School employees who receive a written request should forward it to their line managers and the Data Protection Officer immediately;

10.2.4 have data amended or deleted under certain circumstances where data is inaccurate or to have data completed where data is incomplete by providing a supplementary statement to the School (see also Clause 8);

10.2.5 restrict processing of data if one of the following circumstances applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

10.2.6 Where processing has been restricted, as above, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State and the data subject shall be informed.

10.2.7 where processing is restricted under one of the grounds in Clause 10.2.5, the data shall only be processed with the individual's consent or in relation to the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or the United Kingdom;

10.2.8 an individual who has obtained restriction of processing under Clause 10.2.5 shall be informed by the School before the restriction of processing is lifted;

10.2.9 receive data concerning the individual, which he or she has provided to the School and is processed by automated means, in a structured, commonly used and machine-readable format and to transmit those data to another controller without hindrance from the School;

10.2.10 object to data processing on grounds relating to his or her particular situation unless the School demonstrates compelling legitimate grounds for processing which overrides the interests, rights and freedoms of the individual or for to the establishment, exercise or defence of legal claims; and

10.2.11 not to be subject to a decision based solely on automated decision-making and profiling which produces legal effects concerning him or her or similarly significantly affects him or her unless the decision is based on the individual's explicit consent.

10.3 It is the responsibility of all staff to ensure that any request by an individual under Clause 10.1 is brought to the attention of the Data Protection Officer without undue delay.

10.4 The School may refuse a request by an individual wishing to exercise one of the above rights in accordance with Relevant Data Protection Law.

10.5 The School shall provide information on action taken on a request under Clause 10.1 to the individual within one month of receipt of the request unless the School deems it

necessary to extend this period by two further months where the request is complex and informs the individual of such extension with reasons within one month of receipt of the request.

10.6 If a request under Clause 10.2 is unfounded or excessive, the School may charge a reasonable fee for providing the information or refuse the request.

10.7 When receiving telephone enquiries, we will only disclose Personal Data we hold on our systems if the following conditions are met:

10.7.1 We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

10.7.2 We will suggest that the caller put his or her request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

10.8 Our employees will refer a request to [their line managers and] the Data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

11 NOTIFYING DATA SUBJECTS

11.1 If we collect Personal Data directly from individuals, we will at the time of collection inform them about the processing including:

11.1.1 the identity and contact details for the School and its Data Protection Officer;

11.1.2 the purpose or purposes for which we intend to process those Personal Data;

11.1.3 the types of third parties, if any, with which we will share or to which we will disclose those Personal Data; and

11.1.4 the means, if any, by which individuals can limit our use and sharing of their Personal Data.

11.2 If we receive Personal Data from a source other than the individual we will, except in certain circumstances, provide the individual with the information in Clause 11.1 above at the following times:

11.2.1 within one month of receiving the Personal Data;

11.2.2 if the Personal Data are to be used for communication with the individual, at the time of the first communication to the individual;

11.2.3 if a disclosure to another recipient is envisaged by us, at the time of the disclosure to that recipient.

11.3 A notification in the form of a Fair Processing Notice will be in writing or via a link to our website, unless the individual requests an oral notification.

11.4 We will also inform individuals whose Personal Data we process that the School is the Data Controller with regard to those data and who the Data Protection Officer is.

12 DATA SECURITY

12.1 We will take appropriate security measures against unlawful or unauthorised

processing of Personal Data, and against the accidental loss of, or damage to, Personal Data.

12.2 We will put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction. Personal Data will only be transferred to a Data Processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures.

12.3 School staff can find details of their obligations in relation to security of Personal Data in the Staff Handbook.

12.4 All School staff must:

12.4.1 assist the School in upholding individuals' data protection rights;

12.4.2 only act in accordance with the School's instructions and authorisation;

12.4.3 notify the Data Protection Officer immediately of any Personal Data Breaches, allegations of Personal Data Breaches or suspicions of Personal Data Breaches in accordance with Clause 12.5;

12.4.4 comply at all times with the terms of any agreements with the School and with their responsibilities under Relevant Data Protection Law;

12.4.5 satisfy the School, within a reasonable period following request, of their compliance with the provisions of Clause 12.4.4.

12.5 The School will notify the Information Commissioner's Office of any Personal Data Breaches without undue delay.

12.6 We will maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

12.6.1 **Confidentiality:** only people who are authorised to use the data can access them;

12.6.2 **Integrity:** Personal Data should be accurate and suitable for the purpose for which they are processed;

12.6.3 **Availability:** authorised users should be able to access the data if they need it for authorised purposes. Personal Data should therefore be stored on the School's central computer system instead of on individual computers, tablets or other media.

12.7 Security procedures include:

12.7.1 **Entry controls:** any stranger seen in entry-controlled areas should be reported.

12.7.2 **Secure lockable desks and cupboards:** desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential.)

12.7.3 **Methods of disposal:** paper documents should be shredded. Digital storage devices should be professionally processed and physically destroyed when they are no longer required.

12.7.4 **Equipment:** School staff must ensure that individual monitors do not show confidential information to passers-by and that they log off from their computers, tablets or other devices when left unattended.

12.7.5 **Data storage methods:** measures to store data securely, such as Pseudonymisation or key-coding, will be implemented where appropriate.

12.8 The School shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data-protection principles and to integrate the necessary safeguards into processing activities.

12.9 The School shall implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the processing are processed.

13 REGISTER OF BREACHES

13.1 The School must maintain an accurate and up-to-date register of all Personal Data Breaches. If anyone becomes aware of a data protection breach they must inform the School immediately.

14 DATA PROTECTION OFFICER

14.1 The Data Protection Officer is responsible for ensuring compliance with Relevant Data Protection Law and with this Policy. That post is held by the Head of Finance & Operations, 02036082080, admin@thomsonhouseschool.org. The Data Protection Officer reports to the Head Teacher or the Chair of Governors but fulfils his/her data protection functions independently.

14.2 Any questions about the operation of this Policy or any concerns that the Policy has not been followed should be referred in the first instance to the Data Protection Officer.

14.3 Where a Personal Data Breach has occurred, it will be for the Data Protection Officer to decide whether, under the circumstances and in accordance with Relevant Data Protection Law, the individual concerned must be informed of the breach.

15 USING DATA PROCESSORS

15.1 The School retains the right to engage by written contract any person or organisation, who is not a member of School staff, to process Personal Data on our behalf.

15.2 Data Processors must:

15.2.1 assist the School in upholding individuals' data protection rights;

15.2.2 only act in accordance with the School's instructions and authorisation;

15.2.3 maintain a written record of processing activities carried out on behalf of the School and provide this to the School within [a reasonable period] following request;

15.2.4 notify the School of Personal Data Breaches without undue delay and maintain a register of breaches in accordance with Clause 13;

15.2.5 comply at all times with the terms of any agreements with the School and with their responsibilities under Relevant Data Protection Law;

15.2.6 satisfy the School, within a reasonable period following request, of their compliance with the provisions of Clause 12.4.4.

16 DISCLOSURE AND SHARING OF PERSONAL INFORMATION

16.1 We may share Personal Data we hold with staff at any academy within the School.

16.2 We may also disclose Personal Data we hold to third parties:

16.2.1 if we are under a duty to disclose or share an individual's Personal Data in order to comply with any legal obligation;

16.2.2 in order to enforce or apply any contract with the individual or other agreements; or

16.2.3 to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of child welfare and fraud protection.

16.3 We may also share Personal Data we hold with selected third parties for the purposes set out in the Schedule.

17 REQUESTS FOR INFORMATION

17.1 Requests for information may take the following forms:

17.1.1 Requests for education records.

17.1.2 Freedom of information requests.

17.1.3 Subject access requests.

17.2 Where a person with parental responsibility requests information about a child's educational records then these should be provided.

17.3 If a person makes a request for information under the Freedom of Information Act then the information should usually be provided unless there are some specific concerns about disclosing the information. Common concerns in the school context may be that information relates to other people, is confidential or legally privileged. There is extensive guidance on the ICO website. If a freedom of information request is made and there are any concerns about disclosing information then the Data Protection Officer should be contacted.

17.4 If a person makes a subject access request then they are requesting the personal information that the School has about them. There are exemptions to disclosing some information but these are more limited as a person has a right to know what information is held on them. If a subject access request is made then the Data Protection Officer should be contacted immediately.

18 CHANGES TO THIS POLICY

We reserve the right to change this Policy at any time. Where appropriate, we will notify individuals of those changes by mail or email.

Appendix 1:

Personal data breach procedure:

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by [insert your reporting procedure, e.g. using a dedicated email address, filling out a reporting form, etc.]

The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

- Lost

- Stolen
- Destroyed
- Altered
- Disclosed or made available where it should not have been
- Made available to unauthorised people

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored [set out where you keep records of these decisions on the school's computer system.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:

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

If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach;

- The name and contact details of the DPO;

- A description of the likely consequences of the personal data breach;

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

The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause

- Effects

- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored, on the school's computer system.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Set out the relevant actions you will take for different types of risky or sensitive personal data processed by your school. For example:

Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ClickOnIT to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted

If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families

Schedule Data processing activities

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Contact details	Parents/ guardians Pupils Next of kin	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare School trips and activities management Insurance Supporting learning Monitoring and reporting on pupils' progress Providing appropriate pastoral care Health and safety Employment Provision of paid services including music tuition	Consent; Vital Interests; Public Interest; Contractual Performance; Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies Appropriate community services Youth support services Department for Education (DfE) Third parties designated by the DfE Exam Boards	Until the pupil leaves his/or her School academy
Medical information	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Health and safety	Vital Interests; Public Interest; Legal Obligation	Teaching, support and administrative staff; The NHS/Medical Staff	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Special educational needs	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Health and safety School trips and activities management Supporting learning	Vital Interests; Public Interest; Legal Obligation	Teaching, support and administrative staff; School nurses; The NHS Third parties appropriately chosen by the School Appropriate community services Youth support services Local authority	Until the pupil leaves his/or her School academy
Religious belief	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare School trips and activities management Providing appropriate pastoral care For purposes of the PREVENT scheme	Public Interest; Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School	Until the pupil leaves his/or her School academy
Sexual orientation	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care	Public Interest	Teaching, support and administrative staff Appropriate community services	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
					The NHS/Medical Staff	
Ethnic group	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare	Public Interest; Legal Obligation	Teaching, support and administrative staff Appropriate community services Youth support services Local authority Department for Education (DfE) Third parties designated by the DfE	Until the pupil leaves his/or her School academy
Disciplinary history	Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Developing our understanding of our workforce	Public Interest; Legal Obligation	Teaching, support and administrative staff	Until the pupil leaves his/or her School academy
Vocational learning and qualifications	Employees	Electronic storage Written correspondence	Employment application process Developing our understanding of our workforce Assisting with the development of recruitment and retention policies and practices	Public Interest; Legal Obligation	Teaching, support and administrative staff	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Attendance history	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and assessing the quality of our services Enabling individuals to be paid Developing our understanding of our workforce	Public Interest; Legal Obligation	Teaching, support and administrative staff	Until the pupil leaves his/or her School academy
National curriculum examination results	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Monitoring and reporting on pupil progress	Public Interest; Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies Department for Education (DfE) Third parties designated by the DfE Exam Boards	Until the pupil leaves his/or her School academy
Photographs	Pupils Employees	Electronic storage Physical displays	Administration related to provision of education and pupil welfare Identification of pupils Marketing	Public Interest Consent	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
					Appropriate community services Youth support services Members of the public viewing marketing materials The Police The NHS/Medical Staff	
CCTV footage	Pupils Employees Parents Governors Volunteers Contractors Other third parties	Electronic storage	Administration related to provision of education and pupil welfare Promoting and protecting health and safety	Consent Public Interest	Teaching, support and administrative staff The Police	Until the pupil leaves his/or her School academy
Family information	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care	Public Interest; Legal Obligation	Teaching, support and administrative staff	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Court orders	Pupils Employees Parents	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care	Public Interest	Teaching, support and administrative staff	Until the pupil leaves his/or her School academy
Destination after leaving school	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Monitoring and reporting on pupil progress	Public Interest; Legal Obligation	Teaching, support and administrative staff The local authority and other state bodies Department for Education (DfE) Third parties designated by the DfE Exam Boards	Until the pupil leaves his/or her School academy
Careers guidance	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Monitoring and reporting on pupil progress	Public Interest	Teaching, support and administrative staff Third parties appropriately chosen by the School	Until the pupil leaves his/or her School academy
Education	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Monitoring and reporting on pupil progress	Public Interest; Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
					The local authority and other state bodies Appropriate community services Youth support services Department for Education (DfE) Third parties designated by the DfE Exam Boards	
School Trips	Pupils Employees Volunteers	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Promoting and protecting health and safety Ensuring proper management of school trips and activities	Public Interest Consent Vital Interests	Teaching, support and administrative staff The Police The NHS/Medical Staff	Until the pupil leaves his/or her School academy
Afterschool Clubs	Pupils Volunteers	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Promoting and protecting health and safety Ensuring proper management of after school clubs and activities	Public Interest Consent Vital Interests	Teaching, support and administrative staff Third parties appropriately chosen by the School Appropriate community services	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
					The Police The NHS/Medical Staff	
Employment and Remuneration Details	Employees	Electronic storage Written correspondence	Enabling employees to be paid Developing our understanding of our workforce	Contractual Performance	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies	Until the pupil leaves his/or her School academy
DBS	Employees	Electronic storage	Carrying out a legal requirement to ensure staff are able to work with children and adults	Legal Obligation	Strictly Education who process carry out the DBS check	2 pieces of evidence until the DBS is processed. Passport kept on file for duration of employment
Child Welfare and Safeguarding	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care Promoting and protecting health and safety	Public Interest Vital Interests	Teaching, support and administrative staff The Police The NHS/Medical Staff	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Free School Meal Eligibility	Pupils	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare	Public Interest Legal Obligation	Teaching, support and administrative staff The local authority and other state bodies Department for Education (DfE) Third parties designated by the DfE	Until the pupil leaves his/or her School academy
First Language	Pupils Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care	Public Interest Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies Appropriate community services Youth support services Department for Education (DfE) Third parties designated by the DfE Exam Boards	Until the pupil leaves his/or her School academy

Type of data	Type of Data Subject	Type of processing	Purpose of processing	Lawful Basis for processing	Type of recipient to whom Personal Data is transferred	Retention period
Nationality	Pupils Parents Employees	Electronic storage Written correspondence	Administration related to provision of education and pupil welfare Providing appropriate pastoral care	Public Interest Legal Obligation	Teaching, support and administrative staff Third parties appropriately chosen by the School The local authority and other state bodies Appropriate community services Youth support services Department for Education (DfE) Third parties designated by the DfE Exam Boards	Until the pupil leaves his/or her School academy