Data Protection Policy

Policy Dated:	September 2021
Adopted by Audit Committee:	June 2021
Date of Next Review:	June 2023
Reason for Review/Revision:	Statutory
Publication Scheme	Trust & School websites
Version	02
Lead	CEO

1.0 Introduction

1.1 Extol Trust's Data Protection Policy has been produced to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA), UK GDPR and associated legislation, and it incorporates guidance from the Information Commissioner's Office (ICO). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.2 The DPA gives individuals rights over their personal data and protects individuals from the erroneous use of their personal data.

1.3 Extol Trust processes personal data relating to pupils, parents, staff, Governors, visitors and others, and therefore is a data controller. Extol Trust is registered with the ICO as a Data Controller and will renew this registration as legally required.

1.4 The policy incorporates guidance from the ICO, and outlines Extol Trust's overall approach to its responsibilities and individuals' rights under the DPA 2018.

2.0 Scope

2.1 This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, Extol Trust), Governors, student placements, volunteers, third parties and others who may process personal information on behalf of Extol Trust or any individual schools within the Trust.

2.2 The Policy also covers any staff who may be involved in research or other activity that requires them to process or have access to personal data, for instance as part of a research project or as part of professional practice activities. If this occurs, it is the responsibility of the relevant individual school to ensure the data is processed in accordance with the DPA 2018 and that staff are advised about their responsibilities. In addition, the activity should be referred to the Audit Committee.

3.0 Data Covered by the Policy

3.1 A detailed description of this definition is available from the ICO, however briefly, personal data is information relating to an individual where the structure of the data allows the information to be accessed i.e. as part of a relevant filing system. This includes data held manually and electronically and data compiled, stored or otherwise processed by Extol Trust, or by a third party on its behalf.

3.2 Sensitive personal data is personal data consisting of information relating to:

- Racial or ethnic origin
- Political opinions, religious beliefs or other beliefs of a similar nature
- Membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health condition
- Sexual orientation
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

4.0 The Six Data Protection Principles

4.1 The DPA 2018 requires Extol Trust, its staff and others who process or use any personal information must comply with the six data protection principles.

4.2 The principles require that personal data shall:

1. Lawfulness, Fairness and Transparency - Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met
2. Purpose Limitation - Be obtained for a specified and legitimate purpose and shall not be processed in any manner incompatible with that purpose
3. Data Minimisation - Be adequate, relevant and not excessive for those purposes
4. Accuracy - Be accurate and kept up to date
5. Storage Limitation - Not be kept for longer than is necessary for those purpose
6. Data Security - Be kept safe from unauthorised or unlawful processing and against accidental loss, destruction or damage.
7. Accountability - requires you to take responsibility for what you do with personal data and how you comply with the other principles.
8.

5.0 Roles and Responsibilities

5.1 Extol Trust has an appointed Data Protection Officer (service currently provided by Panormaic Business Operations Services Ltd through a commissioned GDPR service level agreement) to handle day-to-day issues which arise, and to provide members of the Trust with guidance on Data Protection issues to ensure they are aware of their obligations.

5.2 The Local Governing Body of each school within the Trust has overall responsibility for ensuring compliance with all relevant data protection obligations.

5.3 The individual Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All Extol Trust staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Familiarising themselves and comply with the six data protection principles
- Ensuring any possession of personal data is accurate and up to date
- Ensuring their own personal information is accurate and up to date
- Keeping personal data for no longer than is necessary
- Ensuring that any personal data they process is secure and in compliance with Extol Trust's information related policies and strategies
- Acknowledging data subjects' rights (e.g. right of access to ***all*** their personal data held by the School/Trust) under the DPA 2018, and comply with access to records
- Ensuring personal data is only used for those specified purposes and is not unlawfully used for any other business that does not concern the School/Trust
- Obtaining consent with collecting, sharing or disclosing personal data
- Contacting the Headteacher or the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties.

5.5 All new members of staff will be required to complete a GDPR module on GDPRiS as part of their induction and existing staff will be requested to undertake refresher training on a regular basis.

5.6 Pupils of the Extol Trust are expected to comply with policy and procedure appropriate to age.

6.0 Obtaining, Disclosing and Sharing Data

6.1 Only personal data that is necessary for a specific Trust's related business reason will be obtained.

6.2 Pupils' parents are informed about how their data will be processed when they agree to the Data Processing Consent Notice upon registration.

6.3 Upon acceptance of employment at Extol Trust, members of staff also consent to the processing and storage of their data.

6.4 Data must be collected and stored in a secure manner.

6.5 Personal information must not be disclosed to a third party organisation without prior consent of the individual concerned. This also includes information that would confirm whether or not an individual is or has been an applicant, pupil or employee of Extol Trust.

6.6 Extol Trust may have a duty to disclose personal information in order to comply with legal or statutory obligation. The DPA 2018 allows the disclosure of personal data to authorised bodies, such as the police and other organisations that have a crime prevention or law enforcement function. Any requests to disclose personal data for reasons relating to national security, crime and taxation should be directed to DPO service DPO@panoramic.org.uk

6.7 Personal information that is shared with third parties on a more regular basis shall be carried out under written agreement to stipulate the purview and boundaries of sharing. For circumstances where personal information would need to be shared in the case of ad hoc arrangements, sharing shall be undertaken in compliance with the DPA 2018.

7.0 Retention, Security and Disposal

Extol Trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

7.1 Personal information held in paper and electronic format shall not be retained for longer than is necessary. In accordance with principle 2 and principle 4 of the DPA 2018, personal information shall be collected and retained only for business, regulatory or legal purposes. Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use. Personal data in paper format must be

shredded or placed in the confidential waste bins provided when no longer required to be retained. Personal data in electronic format should be deleted and CDs, USB drives etc passed to One IT Services for safe disposal. Hardware should be appropriately degaussed in compliance with our IT service provider contract and that conforms with DPA and GDPR requirements.

7.2 Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to noticeboards/display boards or left anywhere else where there is general access.

7.3 Passwords are changed regularly for electronic devices.

7.4 The screens of office/classroom based machines, laptops etc are locked when not in use or when the member of staff is not in the office/classroom.

7.5 Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

7.6 Recipients responsible for the processing and management of personal data need to ensure that the data is accurate and up-to-date. If an employee, pupil's parent or applicant is dissatisfied with the accuracy of their personal data, then they must inform the Head of School/Headteacher of the individual academies.

7.7 In accordance with Extol Trust's Staff Code of Conduct, staff working from home will be responsible for ensuring that personal data is stored securely and is not accessible to others.

7.8 Personal data that is no longer needed will be disposed of in accordance with the Trust's Retention Schedule. This may include shredding or incineration of paper based records, and deletion of electronic files. We may also use third parties to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees and certification that it complies with data protection law.

8.0 Transferring Personal Data

8.1 Any transfer of personal data must be done securely in line with Extol Trust's Information Security Policy. Transfer of data within schools and the Local Authority use various secure services (Anycomms, S2S) and all staff must ensure they use these facilities for transferring personal data to those organisations.

8.2 Email communication is not always secure and sending personal data via external email should be avoided unless it is encrypted with a password provided to the recipient by separate means such as via telephone.

8.3 Care should be taken to ensure emails containing personal data are not sent to unintended recipients. It is important that emails are addressed correctly and care is taken when using reply all or forwarding or copying others in to emails. Use of the blind copy facility should be considered when sending an email to multiple recipients to avoid disclosing personal information to others.

8.4 Personal email accounts should not be used to send or receive personal data for work purpose.

9.0 Data Subjects Right of Access (Subject Access Requests)

9.1 Under the DPA 2018, individuals (both staff and parents of pupils) have the right to make a 'subject access request' to gain access to personal information that a school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of the personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether an automated decision-making is being applied to their data and what the significance and consequences of this might be for the individual.

9.2 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent. Children under the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on case-by-case basis.

9.3 Subject access requests must be submitted in writing through a Subject Access Request Form which should be sent to the Headteacher. This form is available on the Extol Trust's website at www.extoltrust.co.uk or by emailing enquiries@extoltrust.co.uk If any member of staff receive a subject access request, they must immediately forward it to the Headteacher.

9.4 When responding to subject access requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via telephone or email to confirm the request made

- Will respond without delay and within 1 month of receipt of the request
- Will provide the information without charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

9.5 We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or other individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child.

9.6 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or ask for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.7 In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the Headteacher. If staff receive such a request, they must immediately forward it to the Headteacher.

10.0 Personal Data Breaches

10.1 Extol Trust will make all reasonable endeavours to ensure there are no personal data breaches. However, in the unlikely event of a suspected data breach, Extol Trust will respond to the data security breach quickly and effectively. A breach may arise from a theft, a deliberate attack on Extol Trust systems, unauthorised use of personal data, accidental loss or equipment failure. Any data breach should be reported to the Data Protection Officer at Panoramic Business Operations Services Ltd DPO@panoramic.org.uk and if it relates to an IT incident (including information security), should also be reported to the Headteacher of individual schools and in certain circumstances to our I.T provider – please refer to the Data Breach Reporting Policy for more information.

10.2 Any breach will be investigated in line with the procedures within the Data Breach Reporting Policy. In accordance with that Policy, the School/Trust will treat any breach as a serious issue. Each incident will be investigated and judged on its individual circumstances and addressed accordingly.

11.0 Review of this Policy

The Board of Trustees through its Audit Committee will review this policy biannually year.

It may however review this policy earlier than this if the government produces new regulations, or if it receives recommendations on how this policy might be improved.