KING EDWARD VI ASTON SCHOOL

DATA PROTECTION POLICY

CONTEXT:

- Schools and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature.
- It is the responsibility of all members of the school community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data, and/or need to have access to that data.
- Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office - for the school and the individuals involved. All transfer of data is subject to risk of loss or contamination.
- Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance .
- *The school* collects and uses personal information (referred to in the Data Protection Act as personal data) about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

POLICY STATEMENTS:

- The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- This policy sets out how the school deals with personal information correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation
- This policy applies to all personal information however it is collected, used, recorded and stored and whether it is held on paper or electronically.
- All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

DATA PROTECTION PRINCIPLES

- The Data Protection Act 1998 establishes eight principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;

7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection

PERSONAL DATA:

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

ROLES AND RESPONSIBILITIES:

- The school's Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO) is Mrs W Causer.
- The Headmaster will identify Information Asset Owners (IAOs) for the various types of data being held (e.g pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :
- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.
- Information Asset Owners identified by the Headmaster are:
- SIMS Data – SIMS Data Manager
- Pupil Data – Deputy SIMS Manager
- Staff HR Data – Head's PA
- Biometric Data (Fingerprint data) - AIP
- Assessment and Tracking Data – SIMS Data Manager
- Class and Timetable Data – Assistant Headteacher in Charge of Timetabling.
- Everyone in the school has the responsibility of handling protected or sensitive data 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.

REGISTRATION

- The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner. This registration is managed by the SIRO.

INFORMATION TO PARENTS / CARERS – THE "PRIVACY NOTICE"

- In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held

and the third parties to whom it may be passed. This privacy notice will be passed to parents / carers through a Privacy Notice Statement contained on the school website.

- Parents / carers of students who are new to the school will be provided with the Privacy Notice Statement in the parental information pack which is sent to all new parents.

TRAINING & AWARENESS

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

RISK ASSESSMENTS

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

A risk assessment about the management and handling of data will be completed in September of each academic year by the IAOs and will result in the completion of an Information Risk Actions Form (example below):

Risk ID	**Information Asset affected**	**Information Asset Owner**	**Protective Marking (Impact Level)**	**Likelihood**	**Overall risk level (low, medium, high)**	**Action(s) to minimise risk**

IMPACT LEVELS AND PROTECTIVE MARKING

Government Protective Marking Scheme label	Impact Level (IL)
NOT PROTECTIVELY MARKED	0
PROTECT	1 or 2
RESTRICTED	3
CONFIDENTIAL	4
HIGHLY CONFIDENTIAL	5
TOP SECRET	6

- It is recognised that most student or staff personal data that is used within educational institutions will come under the PROTECT classification.
- However some, eg the home address of a child (or vulnerable adult) at risk will be marked as RESTRICTED.
- The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.
- All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

- Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment

SECURE STORAGE OF DATA

- 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 user status 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.
- All users will use strong passwords which must be changed regularly when prompted by the school system. User passwords must never be shared.
- 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 15 minutes.
- 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). Private equipment (i.e owned by the users) must not be used for the storage of personal data.

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
- the device must offer approved virus and malware checking software and
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

- SLT have access to staff and student data in the case of a Critical Incident. Data can be accessed via tablet devices which use a two stage authentication system with an encrypted data store and remote disable and wipe capabilities.
- The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems.

All paper based Protected and Restricted (or higher) material must be held in lockable storage. Materials relating to Child Protection Incidents will be stored and dealt with as determined by the Child Protection Policy and the BSCB Procedures and Guidance.

CREATION, STORAGE AND USE OF DIGITAL IMAGES OF STUDENTS

- The school will take images of students to record events that have taken place during school time or on extra curricular trips and visits.
- These images are most often taken by the school's photographer.
- A selection of these images will be used for publicity purposes on the school website, publications and advertising.
- Parents are asked at the beginning of each year to consent to images being taken and used for publicity and for the school website.
- Students for whom consent has not been given are 'tagged' in SIMS and a list of these students is stored on a staff accessible school network drive and a copy given to the school's photographer
- Every effort is made to ensure that any images taken do not include students for whom consent has been withheld. Any images that are created inadvertently are permanently deleted.
- At times where the school would like to photograph a student for whom consent has not been given (e.g groups of senior prefects), the school will seek to obtain a 'one off' consent from parents. If this is not granted, students will not be included in the images

- The images created for school are stored in a secure account linked to Google Drive and this data is stored on Google cloud systems in Europe. Only selected members of staff have access to the stored images on the drive.

SECURE ACCESS TO DATA AND SUBJECT ACCESS REQUESTS:

The school recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access.

Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data

Subject Access Requests must be made in writing to the DPO who must discuss the request with the Headteacher before releasing any personal data.

SUBJECT ACCESS REQUESTS PROCEDURES:

- Subject Access Requests must be made in writing to the DPO. There may be a payment of a fee for access of up to £10.00 (for records held on computer) or £50.00 (for those held manually).
- The DPO should discuss the Subject Access Request with the relevant IAO and then the Headteacher before disclosing any personal data.
- Any personal data to be disclosed following a Subject Access Request should be in printed form. The data should be collected from the school office by either:
- The member of staff to whom it concerns or
- The parent(s)/carer(s) of a student.
- The DPO should ensure that the data is signed for upon collection.
- In the case of a parent/carer, the DPO should ensure that ID is sought before the data is disclosed.

SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.
- Data which relates to Child Protection Matters can only be removed from site by the DSP or Deputy DSP in line with BSCB Guidance and Procedures.
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school.
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform.
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the Foundation Office in this event. (n.b to carry encrypted material is illegal in some countries)

DISPOSAL OF DATA

- The school will comply with the requirements for the safe destruction of personal data when it is no longer required. After students have left the school, all student records will be kept for a period of seven years, with files relating to students with Special Educational Needs being held for twenty-five years. All Child Protection records will be kept for twenty-five years.

- The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

AUDIT LOGGING / REPORTING / INCIDENT HANDLING

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs can be accessed if required by the senior ICT technician, the Headmaster or in his absence the Deputy

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy.

In the incidence of a data mishandling or loss, where the data falls into category 3 or above, the person discovering the incident should report the incident to the Headmaster who will establish:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Linked Policies
Child Protection
Privacy Notice for Parents/Carers
E-safety Policy

Governor Approval: July 2015
Date for Review: July 2017

APPENDICES:

Use of technologies and Protective Marking

The following provides a useful guide to the classification of data within school.

	The information	The technology	Notes on Protect Markings (Impact Level)
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

ADDITIONAL ISSUES / DOCUMENTS RELATED TO PERSONAL DATA HANDLING IN SCHOOLS:

USE OF BIOMETRIC INFORMATION

The Protection of Freedoms Act 2012, includes measures that will affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.