DATA PROTECTION AND CCTV POLICY

Policy Statement

Collecting, processing and storing personal information is necessary for the operation of the College as an educational organisation and the College views the correct and lawful handling of personal data as key to its success. This document sets out the obligations of East Kent College ("the College") with regard to data protection, including the use of CCTV and the rights of people with whom it deals with in respect of their personal data under the Data Protection Act 1998 ("the Act").

Details

1. The Data Protection Principles

This Policy aims to ensure compliance with the Act. The Act sets out eight principles with which any party handling personal data must comply. All personal data:

1.1 Must be processed fairly and lawfully;

1.2 Must be obtained only for specified and lawful purposes and shall not be processed in any manner which is incompatible with those purposes;

1.3 Must be adequate, relevant and not excessive with respect to the purposes for which it is processed;

1.4 Must be accurate and, where appropriate, kept up-to-date;

1.5 Must be kept for no longer than is necessary in light of the purpose(s) for which it is processed;

1.6 Must be processed in accordance with the rights of data subjects under the Act;

1.7 Must be protected against unauthorised or unlawful processing, accidental loss, destruction or damage through appropriate technical and organisational measures; and

1.8 Must not be transferred to a country or territory outside of the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

2. Rights of Data Subjects

Under the Act, data subjects have the following rights:

2.1 The right to be informed that their personal data is being processed;

2.2 The right to access any of their personal data held by the College within 40 days of making a request;

2.3 The right to prevent the processing of their personal data in limited circumstances; and

2.4 The right to rectify, block, erase or destroy incorrect personal data.

3. Personal Data

3.1 Personal data includes personal details, academic, employment and administrative history, relevant transactions, CCTV/digital images, photographic images and audio recordings. The College collects and processes information for various purposes, including educational administration, funding, statistical research, health and safety, employment, training, career guidance, equality and disability policy monitoring, for security and insurance reasons. The College only holds personal data which is directly relevant to its dealings with a given data subject. The College holds data in electronic and paper form; data will be held and processed in accordance with the data protection principles and with this Policy.

3.2 Data that may be collected, held, processed and stored by the College (Included but is not limited to):

4. Processing Personal Data

All information concerning individuals is treated in the strictest of confidence and will not be released unless the individual gives consent. There are some exceptions which are outlined below.

4.1 Student's personal data may be disclosed within the College for administrative purposes. Personal data may be passed from one area to another in accordance with the data protection principles and this Policy. Under no circumstances will personal data be passed to any area or any individual within the College that does not reasonably require access to that personal data with respect to the purpose(s) for which it was collected and is being processed. Unless there is an opt out, the College shall pass the individual's name, registration number, area and course detail to the Students' Union who collects the information for various administrative, marketing and event purposes.

Personal data shall also be used by the College in meeting any and all relevant obligations imposed by law and for its own security, disciplinary or insurance reasons. The data will be used for administrative purposes as outlined above while the student is at College and after

course completion for marketing purposes. Personal data shall not be passed to external parties without the student's agreement. The College appoints external and internal auditors who have access to student's personal data but this information is treated in the strictest of confidence.

4.2 Staff data is used by the College to administer and facilitate efficient transactions with third parties including, but not limited to, its partners, associates, affiliates and government agencies and to efficiently manage its employees, contractors, agents and consultants.

4.3 The College has certain statutory obligations under which it may be required to pass personal information relating to an individual to external agencies. Where possible the individual will be informed about these disclosures but in some cases it is not possible to do this. The Act allows organisations to disclose information to relevant bodies for law enforcement and collection of taxes.

4.4 Unless permission has been given for additional information to be provided, the only information that will normally be released to a third party (other than funding agencies or law enforcement agencies) while a student is here is:

- the fact the individual is a student or employee of the College;
- whether full or part time;
- the date started and the date expected to leave;

4.5 The College will use appropriate security measures to prevent unauthorised disclosure. The College shall ensure that:

- All personal data collected and processed for and on behalf of the College by any party is collected and processed fairly and lawfully;
- Data subjects are made fully aware of the reasons for the collection of personal data and are given details of the purpose for which the data will be used;
- Personal data is only collected to the extent that is necessary to fulfil the stated purpose(s);
- All personal data is accurate at the time of collection and will endeavour to keep it accurate and up-to-date while it is being held and / or processed;
- No personal data is held for any longer than necessary in light of the stated purpose(s);
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data;
- All personal data is transferred using secure means, electronically or otherwise;
- No personal data is transferred outside of the UK or EEA (as appropriate) without first ensuring that appropriate safeguards are in place in the destination country or territory; and

- All data subjects can exercise their rights set out above in Section 2 and more fully in the Act.

4.6 If a student or employee reference is requested from the College, written consent is required from the individual to supply the information. The fact that the name of the tutor and College has been given to a third party for the purpose of a personal, academic or employment reference, does not enable the College to consider that consent for the disclosure of personal information in the form of a reference has been given.

4.7 Data release to parents, guardians or legal guardians will not normally be made without written consent, unless the individual is aged under 18 years of age and/ or is subject to a care programme. This will be the case from the academic year of the student's 18th birthday. Students aged 16 and 17 years old can inform the College of their request to withhold information to parents, guardians or legal guardians but will need to evidence good reason for their request with Student Support Services at the College.

5. Data Protection Procedures

5.1 The College shall ensure that all of its employees, contractors, agents, consultants, partners or other parties working on behalf of the College comply with the following when processing and / or transmitting personal data:

- All personal data will be as an attachment to an email and not in the email message
- Personal data may not be transmitted over an unsecured network
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
- All hardcopies of personal data should be stored securely in a locked box, drawer, cabinet or similar;
- All electronic copies of personal data should be stored securely using passwords and suitable data encryption, where possible on a drive or server which cannot be accessed via the internet; and
- All passwords used to protect personal data should be changed regularly and should not use words or phrases which can be easily guessed or otherwise compromised.
- Use of personal devices by employees is permitted to access personal data but not to store it; further in this instance the procedures of this Policy must be adhered to at all times.

- Personal data that is in paper format will be disposed of via confidential waste and removed/destroyed by a licenced contractor.
- All records will be retained in accordance with the College's Records Retention Policy and schedule.

6. Use of CCTV

CCTV systems are in use throughout the College's campuses. CCTV systems operate to assist with the security of the College's staff, students, visitors and physical assets.

6.1 The objectives of CCTV systems at the College are to:

- Protect the College's buildings and physical assets
- Assist in identification, apprehension and prosecution in relation to actual or suspected crime

Provide and operate the system in a manner which is consistent with the respect for privacy of all individuals.

6.2 The College will ensure where possible that staff, students, visitors and the general public accessing the site are made aware of the presence of the system and its ownership by the appropriate notices and signage.

6.3 CCTV monitoring systems may be used to focus on particular people by directing cameras at an individual's activities. This may include an operative (when present) looking out for particular individuals or examining recorded CCTV footage to find out about persons captured on the footage, such as detecting and identifying those involved in illegal activity or potential witnesses to an activity captured on the CCTV.

6.4 All means of recording images belong to, and remain the property of the College. Copyright of images recorded by CCTV cameras are the property of the College.

6.5 CCTV images will not be retained for longer than 25 days. While retained, the images will be appropriately secured. The exception to this is where images are copied onto another device for use as evidence by the College for disciplinary procedures or as evidence by the Police or Courts. Where this is the case, the images will be held for a maximum of a calendar year by the College. If images are transferred from the CCTV system, the location to which they are transferred must be documented and a signature must be obtained for the transfer.

6.6 Disclosure of images will only be made in the following cases:

- To the Police or other law enforcement agencies where the images recorded could assist in in a specific criminal enquiry and/or the prevention of a crime.
- To Prosecution agencies
- To authorised legal representatives

- To members of staff involved with College disciplinary procedures

6.7 All persons accessing and monitoring CCTV will be trained and authorised.

7. Organisational Measures

The College shall ensure that the following measures are taken with respect to the collection, holding and processing of personal data:

- A designated officer ("the Data Protection Officer") within the College shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the Act.
- All students, employees, contractors, agents, consultants, partners or other parties working on behalf of the College are made fully aware of both their individual responsibilities and the College's responsibilities under the Act and shall be either provided a copy of this Policy or directed to a copy available on the College website.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the College handling personal data will be appropriately trained to do so.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the College handling personal data will be appropriately supervised.
- Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed and internal data audits carried out at least every three years.
- All employees, contractors, agents, consultants, partners or other parties working on behalf of the College handling personal data will be bound to do so in accordance with the principles of the Act and this Policy by contract. Failure by any employee to comply with the principles or this Policy shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply with the principles or this Policy shall constitute a breach of contract. In all cases, failure to comply with the principles or this Policy may also constitute a criminal offence under the Act.
- All contractors, agents, consultants, partners or other parties working on behalf of the College handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the College arising out of this Policy and the Act.
- Where any contractor, agent, consultant, partner or other party working on behalf of the College handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the College against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.
- Upon terminating service to the College all employees, contractors, consultants, partners or other parties working on behalf of the College warrant that they have returned and destroyed all duplicate copies of any personal data they have held whilst undertaking activities on behalf of

the College and will not use, retain or transfer any such information collected whilst in the services of the College.

- Upon terminating service to the College all employees, contractors, consultants, partners or other parties working on behalf of the College will have their College email account and access to the College network terminated with immediate effect.
- A data subject must inform the College in writing if they wish to exclude their personal data from particular data processing provisions contained within this Policy, being mindful that complete exclusion would result in the individual being unable to continue as an employee or student since the College would be unable to carry out basic operations. College contact details are contained within section 7 below.

8. Access by Data Subjects

9.1 A data subject may make a subject access request ("SAR") at any time to see the information which the College holds about them.

- Subject Access Requests must be made in writing, accompanied by the correct fee.
- The College currently requires a fee of £10 (the statutory maximum) with all SARs. A fee of £2 shall be required for access to a credit file.

9.2 Upon receipt of a SAR and the requisite fee, the College shall have a maximum period of 40 days within which to respond. The following information will be provided to the data subject:

- Whether or not the College holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

9.3 If an individual wishes to exercise their rights under the Act they should contact the Data Controller at the following email address: corporate.services@eastkent.ac.uk or in writing to the Corporate Services Office, East Kent College, Ramsgate Road, Broadstairs Kent CT10 1PN - www.eastkent.ac.uk