

DATA PROTECTION POLICY

INTRODUCTION AND SCOPE

Collecting and using personal information is vital for the operation of EKC Group as an educational organisation and the Group views the correct and lawful handling of data about individuals as key to its success.

The EKC Group is committed to complying with the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 which aims to make organisations fully accountable for the data that they process about individuals. This policy sets out the steps that the Group takes to demonstrate that it has robust and effective processes in place to protect individuals' data.

The policy applies to:

- EKC Group staff, Governors, contractors, consultants, trainee teachers, volunteers and third party agents;
- Students where they are College Apprentices or are working for the EKC Group in a paid or unpaid capacity.

DETAILS

1. Definitions

1.1 Consent

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

1.2 Data

Any data which identifies a living individual (subject). There are two categories of data in relation to individuals:

Personal data is any data which could be used to identify a living individual e.g. name, contact details (address, telephone number, email address), date of birth, age, gender, bank details, next of kin, photographs, CCTV images, audio recordings.

**Special category personal data is any data which an individual may not wish others to be aware of e.g. ethnicity/nationality, mental/physical health, criminal convictions, socio economic status, personal life (marital status, pregnancy/maternity, interests/hobbies), genetic/biometric profile*, sexuality*, faith/religion*, membership of Trades Unions* Items marked *may not be processed by EKC Group unless the student/employee gives their consent for this data to be processed for specific and lawful purposes. In most cases, the EKC Group has to process special category personal data to meet vital interests and legal obligations but will always seek explicit consent for processing.

**Special category data was known as sensitive data under the Data Protection Act 1998

1.3 Data Breach

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.

1.4 Data Controller

A public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. EKC Group is the Data Controller in relation to the processing of data for Group purposes.

1.5 Data Processor

A person, public authority, agency or other body which processes personal data on behalf of the controller e.g. a subcontractor

1.6 Data subject

An identified or identifiable, living person

1.7 Processing

Any activity in relation to personal data e.g. collection, storage, adaptation, retrieval, consultation, use, disclosure by transmission, erasure, destruction etc.

1.8 Pseudonymisation

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information e.g. use of an encryption code.

2. The Data Protection Principles

The GDPR sets out six principles with which any party handling data about individuals must comply. The Regulation states that data shall be:

1. processed fairly, lawfully and transparently;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. adequate, relevant and limited to what is necessary;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate...are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
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

EKC Group has published a [Data Protection Charter](#) showing how it makes every reasonable endeavour to practically and operationally uphold these principles. All staff and individuals working on behalf of EKC Group are expected to familiarise themselves and work in accordance with the charter.

3. Lawful basis for processing data

The GDPR imposes a requirement for organisations to determine a lawful basis for processing data to include at least one of the following criteria:

- Consent – where an individual has given their consent via clear, affirmative action e.g. providing a signature or ticking a box;
- Performance of a contract e.g. an employment contract, learning agreement etc;
- Legal obligations – because the law requires the data to be processed e.g. for the purposes of HMRC payments;
- Vital interests – to protect the individual in the case of an emergency;
- Public interest or exercise of official authority e.g. provision of statistical returns, to comply with government funding requirements etc;
- Legitimate interests – does not apply to public authorities and the Group cannot therefore rely on this basis.

EKC Group has published a Register of Processing Activities for staff and students which details the type of data which is processed, the lawful basis for processing, how the data is stored and who the data may be shared with/accessed by. The Group publishes a separate retention schedule which details how long data is retained for.

4. Data Protection Standards

Staff and any individuals officially appointed to work on behalf of EKC Group must abide by the principles outlined in this policy and the data protection charter. Specifically, they must ensure that:

- All personal data collected and processed for and on behalf of EKC Group 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; EKC Group must 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;
- Data is not unnecessarily duplicated or distributed;
- Data protection risks will be considered and mitigated by carrying out a Data Protection Impact Assessment in certain circumstances (see section 7).
- 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.

EKC Group shall ensure that the following measures are taken with respect to the processing of personal data:

- A designated data protection officer (DPO) within the Group shall be appointed with the specific responsibility of overseeing data protection and ensuring compliance with the legislation. The DPO will be a qualified GDPR Practitioner.
- All staff and other parties working on behalf of EKC Group will be made fully aware of both their individual responsibilities and the College's statutory responsibilities and shall be either provided a copy of this policy or directed to a copy available on the EKC Group's website.
- All staff or other parties working on behalf of EKC Group who process personal data will be appropriately trained to do so. New staff will undertake training in data protection when they commence employment and participate in refresher training at least every three years after that.
- All staff and other parties working on behalf of EKC Group who process 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 staff or other parties working on behalf of EKC Group who process personal data will be bound to do so in accordance with data protection legislation and this Policy by contract. Failure by an employee to comply shall constitute a disciplinary offence. Failure by any contractor, agent, consultant, partner or other party to comply shall constitute a breach of contract. In all cases, failure to comply may also constitute a criminal offence under data protection legislation.
- All contractors, agents, consultants, partners or other parties working on behalf of EKC Group who process 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 EKC Group arising out of this Policy and data protection legislation. The Group will carry out due diligence on all external parties prior to engagement to seek assurances in respect of compliance with data protection legislation.

- Where any contractor, agent, consultant, partner or other party working on behalf of EKC Group fails in their obligations under this Policy that party shall indemnify and hold harmless EKC Group against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.
- Upon terminating service to EKC Group all employees, contractors, consultants, partners or other parties working on behalf of the EKC Group warrant that they have returned and destroyed all duplicate copies of any personal data they have held whilst undertaking activities on behalf of the Group and will not use, retain or transfer any such information collected whilst in the services of the Group.
- Upon terminating services to EKC Group all employees, contractors, consultants, partners or other parties working on behalf of the Group will have their work email account and access to the Group network terminated with immediate effect.
- A data subject must inform the Group 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 Group would be unable to carry out basic operations.

5. Processing Personal Data

- 5.1 EKC Group 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, security and insurance reasons. The Group only holds personal data which is directly relevant to its dealings with a given individual. EKC Group holds data in electronic and paper form; data will be held and processed in accordance with legislative requirements and with this policy. All information concerning individuals is treated in the strictest of confidence and will not be released unless the individual gives consent.
- 5.2 Student's personal data may be disclosed within EKC Group for administrative purposes. Personal data may be passed from one area to another in accordance with legislation and this policy. Under no circumstances will personal data be passed to any area or any individual within the Group 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, EKC Group 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.

- 5.3 Personal data shall also be used by EKC Group 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 EKC Group appoints external and internal auditors who have access to student's personal data but this information is treated in the strictest of confidence.
- 5.4 Staff data is used by EKC Group 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.
- 5.5 EKC Group 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. Personal data may be disclosed without an individual's permission in the case of protecting an individual's or others' vital interests, to support criminal investigations and in matters of national security.
- 5.7 Data release to parents, carers or guardians who are detailed on a student's records will normally be made without written consent of the student unless the student is aged 18 or over. Where students are aged 18 and over and have an Education, Health and Care Plan (EHCP) or where they do not have the capacity to make their own decisions, parents/carers and guardians who are authorised to act on behalf of the student may have access to the student's data without the student's consent. Parents, carers and guardians may have access to their child's learning and progress records through the Parent Portal. Staff must always check whether they are permitted to share information with a parent, carer or guardian.

6. Roles and responsibilities

All individuals identified in the scope of this policy have a responsibility to work in accordance with the policy and legislative requirements and ensure that they have sufficient training and competence on data protection. However, the following roles have specific accountabilities:

Executive and Governors

- Ensures that adequate resources are available for the implementation of data protection policies and procedures;
- Champions data protection and models good practice.

Data Protection Officer (DPO)

- Informs and advises the College and its staff about obligations to comply with the GDPR and other data protection laws;
- Monitors compliance with the GDPR and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments; training staff and conducting internal audits;
- Advises and guides on the application of policy and procedure;
- To be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc);
- Reporting data breaches to the ICO;
- Advising the Executive and Governors about their obligations under data protection legislation;
- Maintains and updates knowledge and expertise on data protection sufficient to effectively fulfil the role of DPO.

Head of IT

- Ensures that appropriate and adequate technical measures are in place to safeguard the security of data;

Head of HR

- Takes the lead on information processed with regard to staff and assures the security and integrity of personal data.

Assistant Principal/College Services Manager

- Takes the lead on information processed with regard to students. This includes examinations data, academic performance and disciplinary procedures;
- Arranges for the archiving of student data and the disposal of data at the expiry of the data retention period.
- Reporting data breaches to the ICO when the DPO is absent.

7. Data Protection Impact Assessments

The purpose of a Data Protection Impact Assessment (DPIA) is to consider and mitigate the risks associated with processing personal data. The EKC Group will conduct a DPIA in all the following circumstances:

- When introducing new systems and processes
- When making changes to existing systems and processes which involves a higher level or risk for personal data
- When processing 'high risk' data e.g. about vulnerable individuals, those with criminal convictions etc.
- When introducing new technologies that involve personal data processing

A DPIA form will be completed by the member of staff responsible for the area/project and sent to the DPO. There must be a clear action plan to identify and address any issues with regard to data protection. These actions must be completed and signed off by the respective Head of area/Senior person before any data processing is undertaken. The DPO will provide advice and guidance on carrying out DPIAs.

8. Data Privacy notices

In all cases, the EKC Group will publish data privacy notices (also known as fair processing notices) at each stage of processing to advise individuals:

- What data will be collected
- Why the EKC Group needs it

- The legal basis for processing the data
- Data Subject's rights
- Who will have access to the data
- How long the data will be retained for
- Contact Details for the DPO

9. Data breaches

A breach of data is defined as a security incident that has adversely affected the confidentiality, integrity or availability of personal data. This could include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The EKC Group will comply with its statutory duty to report all data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Staff must follow the [Data Breach procedure](#) in all such circumstances. Failure to notify the ICO about a breach could result in significant penalties i.e. a maximum fine of €20,000,000 or 4% of annual turnover.

10. Data Security

All staff and any individuals working on behalf of the EKC Group must ensure the security of personal data by working in accordance with this policy and the data protection charter. A separate [IT Security Procedure](#) provides specific details about the measures taken by IT staff to protect the security of data.

11. Data Retention

EKC Group undertakes to dispose of data upon expiry of the data's retention period. There is a separate [Data Retention and Archiving procedure](#) in place which all staff need to comply with.

12. Subject Access Requests

A data subject may make a subject access request ("SAR") at any time in relation to the information which the College holds about them. Subjects must submit their request in writing to DPO@eastkent.ac.uk and will be required to validate their identity before any data is released. Responses will be provided within 20 calendar days. There is a separate [Subject Access Request Procedure](#) which provides details about the process. Authorised third parties who may make a Subject Access Request without the consent of the individual for the purposes of fulfilling a legal or public interest purpose e.g. investigating and preventing crime, must complete the relevant form. Staff must follow the [Disclosure of Personal Data to third parties procedure](#) in all such circumstances.

13. Complaints

If individuals have any complaints about how the Group is protecting their data, they must submit the complaint to DPO@eastkent.ac.uk. If the complaint is not resolved to the individual's satisfaction, they may refer the matter to the ICO:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
Telephone: 08456 30 60 60 or 01625 54 57 45 www.ico.gov.uk

Related policies, procedures and forms

- Data Protection Charter
- Data Breach procedure
- CCTV procedure
- IT Acceptable Use policy
- IT Security procedure
- Image Use procedure

- Subject Access Request procedure
- Disclosure of Data to Third Parties procedure
- Student References procedure
- Records Retention and Archiving procedure
- Register of Processing Activities (students and staff)
- Home, Remote and Mobile Working procedure
- Data Protection Impact Assessment form