DATA PROTECTION POLICY

INTRODUCTION AND SCOPE

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

The 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:

- Group staff, Governors, contractors, consultants, trainee teachers, volunteers and third party agents;
- Students where they are College Apprentices or are working for the 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 the Group unless the student/employee gives their consent for this data to be processed for specific and lawful purposes. In most cases, the 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 6 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

The 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 the Group are expected to familiarise themselves and work in accordance with the charter and with relevant policies and procedures.

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.

The 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 Records 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 the 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 the 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. This will be achieved via publication of Privacy Notices;
- 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; the 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 without first ensuring that appropriate safeguards are in place in the destination country or territory. This will be determined by undertaking a Data Protection Impact Assessment.

The 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 work towards being a qualified GDPR Practitioner.

- All staff and other parties working on behalf of the Group will be made fully aware of both their individual responsibilities and the Group's statutory responsibilities and shall be either provided a copy of this policy or directed to a copy available on the Group's website.

- All staff or other parties working on behalf of the 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 the 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 the 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 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 the Group arising out of this Policy and data protection legislation.

- Where any contractor, agent, consultant, partner or other party working on behalf of the Group fails in their obligations under this Policy that party shall indemnify and hold harmless the Group against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

- Upon terminating service to the Group all employees, contractors, consultants, partners or other parties working on behalf of the 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 the 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.

5. Processing Personal Data

5.1 The 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. The 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 the 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, the 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 the 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 on roll and after course completion for marketing purposes. Personal data shall not be passed to external parties without the student's agreement unless the purpose is to fulfil a statutory duty. The 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 the 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.

6. Consent

6.1 Data release to parents, carers or guardians who are detailed on a student's records for emergency/next of kin contact will normally be made without the consent of the student unless:

- the student is aged 18 when they commence College or until the end of the academic year in which the student reaches the age of 18;
- the student notifies the Group of a valid reason for not releasing their data;
- the Group has been advised by its Safeguarding staff, Social Services or other official agency of a reason not to do so.

Details shared with parents, carers or guardians will include behaviour, attendance, academic progress, learner support, wellbeing and other details required to keep the student safe whilst they are at college. Parents, carers and guardians may have access to their child's learning and progress records through the Parent Portal.

6.2 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 must provide legitimate evidence where this is the case.

6.3 Staff must always check whether they are permitted to share information with a parent, carer or guardian and must not share data in circumstances where the safety and welfare of a student may be compromised. Staff will always verify the identity of the requestor before releasing any data. This will be done by ensuring the contact number or email address of the requestor matches that on the system before responding. If the caller's telephone number does not match that on the system, staff will verify identity by asking the caller to verify 3 personal identifiers from the list below:

Student's Date of Birth
Student's phone number
Student's email address
The course the student is enrolled on
Student's first line of address
Student's postcode

Callers must answer 3 of the above personal identifier questions correctly for staff to release data to them. Wherever possible, we will encourage parents, carers and guardians to use ProPortal to make any enquiries about their child's course or progress.

6.4 The Group will not share application, interview or other information about a prospective student before they enrol, unless the student has consented.

6.5 The Group will always seek consent from students and staff for the purpose of using their data for internal or external marketing purposes.

6.6 The Group has certain statutory obligations under which it may be required to pass personal information relating to a data subject to external agencies. Where possible the data subject will be informed about these disclosures but in some cases it is not possible to do this. Personal data may be disclosed without a data subject's consent in the case of protecting a data subject's or others' vital interests, to support criminal investigations and in matters of national security.

7. Data Subjects' Rights

Data Subjects have the following rights under data protection legislation. These rights are explained below together with details of how we will ensure these rights are met. EKC Group undertakes to fulfil any rights exercised by a data subject within 1 month of the request being made.

7.1 Right to be informed

The Group will inform data subjects about the data that it processes and will do this via Privacy Notices published on the Group's website. The notices detail:

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

7.2 Right of access

Data subjects have the right to obtain confirmation that their data is being processed and the right to submit a data subject access request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing or obtain copies of their records for other purposes. Data Subject Access Requests can be made by completing and submitting this form. Some data may be subject to an exclusion under GDPR and the Data Protection Act 2018 and cannot therefore be released to the data subject even though they may have requested it.

7.3 The right to rectification

Data subjects may request that inaccurate or incomplete personal data is rectified.

7.4 The right to erasure (right to be forgotten)

Data subjects have the right to request the erasure (deletion) or removal of personal data where there is no lawful basis for its continued processing, in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent

- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services e.g. selling goods or services on-line; to a child
- In a marketing context, where personal data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the personal data must not be processed for such purposes.

EKC Group has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes;
- The exercise or defence of legal claims;
- Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so;
- Where personal data has been made public within an online environment. We may be able to exercise the right to erasure where content has been downloaded or re-shared;
- Where personal data has been used for printed materials such as marketing leaflets and prospectuses and these have already been distributed.

The Group will not process data erasure requests from third party websites due to the security implications involved.

7.5 The right to restrict processing

Data subjects have the right to request that the Group blocks processing of their personal data unless that restriction means that EKC Group is unable to fulfil a legal or contractual obligation or there is another lawful basis for processing. We will restrict processing of personal data in the following circumstances:

- Where an individual disputes the accuracy of the personal data
- Where an individual has objected to the processing and we are considering whether our legitimate grounds override those of the individual
- Where processing is unlawful

7.6 The right to data portability

Data subjects have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

We are not required to adopt or maintain processing systems, which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual.

7.7 The right to object

Data subjects have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing (we cannot refuse an objection to processing for direct marketing purposes)
- Processing for purposes of scientific or historical research and statistics.

We will not stop processing the data subject's data if the processing is for the establishment, exercise or defence of legal claims or where we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject.

8. 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 Group 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;
- Advises and guides on the application of Data Protection Impact Assessments;
- 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.

Director of IT

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

Director 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.

Directors/Managers/Heads

- Ensures that their staff are compliant with all data protection policies and procedures and that they are appropriately trained.

9. 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 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. Where the risks are deemed to be too high, data processing will not take place until the risks have been mitigated. The DPO will provide advice and guidance on carrying out DPIAs.

10. 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 Group will comply with its statutory duty to report all relevant data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. Staff must follow the Data Security 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.

11. Data Security

All staff and any individuals working on behalf of the 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. The increasing trend in flexible working patterns which involves remote and home working means that there is a greater risk to the security of personal data. Staff must comply with the Group's Remote and Home Working procedure in all cases. EKC Group has Cyber Essentials Plus accreditation which helps to demonstrate compliance with the technical measures required to protect personal data.

12. 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 and a Records Retention Schedule in place which all staff need to comply with.

13. Contact details

If data subjects wish to contact EKC Group to query the processing of their data or to make a complaint , they must submit their query/complaint to DPO@eastkent.ac.uk If the query or 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 Protection Impact Assessment form
- Data Security Breach procedure
- Data Subject Access Request procedure
- CCTV procedure
- Image Use and Audio Recording Procedure
- IT Acceptable Use policy
- IT Security procedures
- Records Retention and Archiving procedure and Schedule
- Register of Processing Activities (students and staff)
- Remote and Home Working procedure
- Student References procedure