

KMPF INFORMATION SHARING AND DATA PROTECTION POLICY

This policy has been constructed to ensure that the Kent and Medway Progression Federation complies with the requirements of the Data Protection Act 1998 ('the Act') and the General Data Protection Regulation (GDPR) from May 2018.

1. Introduction

Kent and Medway Progression Federation collects, processes and stores information about the pupils and schools with whom we work in order to administer and evaluate the project.

When handling such information, KMPF, and all staff or others who process or use any personal information on its behalf, must comply with the Data Protection Principles set out in the Data Protection Act 1998 ('the Act') and, from May 2018, the GDPR. In summary, these state that personal data will be:

- i. processed fairly and lawfully
- ii. obtained for specified and lawful purposes and not further processed in a manner incompatible with those purposes
- iii. adequate, relevant and not excessive
- iv. accurate and, where necessary, up to date
- v. kept for no longer than necessary
- vi. processed in accordance with data subjects' rights
- vii. protected by appropriate security
- viii. not transferred to a country outside the European Economic Area without adequate protection

KMPF, and all staff or others who process or use any personal information, must ensure that they follow these principles at all times. This policy sets out the ways in which we will ensure that these principles are put into practice.

2. Data Controller

- 2.1 KMPF is hosted by Canterbury Christ Church University as the lead banker institution. As a result, all information hosted and processed by KMPF regarding employees, students, and other data subjects for academic, administrative and commercial purposes must be in accordance with the hosting institution's Data Protection Policy, which in turn, needs to comply with the Act.
- 2.2 The Act applies to data held in manual paper files as well as on electronic systems. To comply with the Act, information must be collected and used fairly, stored safely and only disclosed lawfully to a third party.
- 2.3 This policy has been reviewed by the Data Protection Officer for Canterbury Christ Church University, as the hosting organisation for KMPF.

3. Policy Aims

- 3.1 This policy has been constructed to meet the commitment to item v.ii *protected by appropriate security* listed above. It is concerned with the handling of information related to KMPF and the processes outlined below:
 - a) **The submission of information** (including emails, forms, folders, invoices) to the KMPF Support Team¹ electronically, in person or through postal delivery;
 - b) **The storage of information** held in manual paper files as well as on electronic systems;
 - c) **The distribution of this information to third parties** either in person (e.g. through the distribution of reports at meetings), by post or electronically (e.g. by e-mail or through a designated website);
 - d) **The disposal of information;**
 - e) **KMPF policy towards employees with access to information** related to the project.

¹ Referred to throughout this document as all KMPF Support Team offices and employees located at the Governor's House campus respectively.

- 3.2 The policy also details the responsibilities of all parties: KMPF and partner Higher Education Institutions (HEIs), partner Further Education Colleges (FECs) and partner schools who from this point forward will be referred to under the collective term 'KMPF partners'.
- 3.3 While all KMPF partners will sign their agreement to this policy, this in no way overrides alternative agreements that might be made between individual partners. The aim is always to ensure that information collected and distributed by KMPF is secure at all times.

4. The nature of information collected by KMPF

- 4.1 KMPF collects information about the students participating in KMPF outreach activities in order to track the proportion who subsequently enter higher education. This enables us to evaluate and improve the programme, as well as report to local funders and relevant national bodies.
- 4.2 Personal information will be collected through student baseline forms, post-activity questionnaires, activity attendance records or any other form containing the following details:
- a) Full Name
 - b) Date of Birth
 - c) Gender
 - d) School Name
 - e) Parental Educational background
 - f) Ethnicity
 - g) Postcode
 - h) Disability
 - i) First Generation HE
 - j) Qualitative baseline data regarding participants' attitudes and perceptions of education, particularly higher education.

5. Obtaining consent

- 5.1 KMPF will ask participating schools / academies / colleges to explain to pupils and parents:
- Why their data is being requested;
 - How long their data will be stored for;
 - The need for data sharing between KMPF delivery partners (for example, to store student information on the database administered by the Higher Education Access Tracker service);
 - The essential need for data sharing with official custodians of education data including the Higher Education Statistics Agency (HESA), The Universities and Colleges Admissions Service (UCAS), the Department for Education (DfE), the Office for Students (OfS), and other agencies (for research purposes only);
 - The need for data to be transferred in both directions from the school / academy / college to KMPF, and in reverse (for example, to advise schools which of their students fall within targeting criteria);
 - How to obtain access to personal data or raise queries about how it is held.
- 5.2 Where consent is the lawful condition for processing the data, it will remain the responsibility of participating schools / colleges / academies to gain appropriate consent from students and parents **before collecting or providing any student information to KMPF, or allowing students to participate in KMPF activities.** The nature of consent required (e.g. parental consent / student consent) may vary over time, and will be dependent on the age of the student; in all cases schools must comply with the most up-to-date guidance set out by the Information Commissioner's Office (www.ico.org.uk). Any changes to these requirements will be reflected within the Partner Schools' Area of the KMPF website at www.kmpf.org.
- 5.3 Where consent is the lawful condition for processing the data, schools / academies / colleges will be asked to keep hard copies of consent forms (which KMPF may ask to see) and provide written confirmation to KMPF that they have the necessary consent to share personal information with KMPF for any students whom they wish to participate in KMPF activities.
- 5.4 Parents and students can opt out of student data recording and data sharing at any time if they wish to do so. If consent is not given, then information must not be collected or passed to KMPF. If a participant (or parent) withdraws consent, it is the responsibility of the school / academy / college to inform KMPF so that we can remove their details from our records and request their removal from the HEAT database.

6. The submission of information to the KMPF Support Team office

This section concerns the submission of information either electronically, by post or in person to the KMPF Support Team.

KMPF partners should be aware that the security and safe storage of information specific to KMPF is the responsibility of the submitting KMPF partner. This responsibility will be maintained up to the point that written acknowledgement of receipt (either in receipt or e-mail form) of the information submitted is issued by the KMPF Support Team.

a) Postal submission of KMPF information

- i) A KMPF partner wishing to submit information including (e.g. Student Name, Date of Birth, School, parental background in HE) by post will do so using a system that provides a written record of delivery (e.g. Royal Mail Special Delivery or Recorded Signed For).
- ii) Under no circumstances should information be submitted by regular post by a KMPF partner.
- iii) A KMPF partner, when submitting information by post, will make sure that it is clearly labelled to show which College, Academy or School has sent it and will include the name of the sender.

b) Submission in person of KMPF information

- i) Whilst recorded delivery is KMPF's preferred method of submission, KMPF partners will continue to submit information in person to the KMPF Support team where appropriate.
- ii) However, KMPF partners must be aware that the responsibility for this information will remain with the submitting institution up to the point that written acknowledgement of receipt (either in receipt or e-mail form) of the information submitted is issued by the KMPF offices. This responsibility includes maintaining the secure storage of this information in compliance with the Data Protection Act at all times (including in transit).

c) Electronic submission of KMPF information

- k) Information may only be submitted electronically through the use of an approved secure system, to be advised through the KMPF Support Team. For information please contact kmpf@canterbury.ac.uk.
- l) Information is also transferred from the KMPF Support Team back to schools / academies and colleges through the use of an approved secure system, to be advised through the KMPF Support Team. For information please contact kmpf@canterbury.ac.uk.

7. The receipt of information by KMPF offices and KMPF partners

The following steps outline the process to be applied when information is received and stored by KMPF.

- a) As soon as information is received by the KMPF offices, a written acknowledgement of receipt will be issued to the submitting KMPF partner. Depending on the method of submission this will either take the form of a written receipt (if the information is handed in person) or a confirmation by e-mail.
- b) Both the submitting and receiving party will keep a copy of this receipt for future reference.
- c) The KMPF partner will be responsible for the secure storage of any information related to the KMPF project prior to its submission to KMPF offices.
- d) Once received, it will be the responsibility of KMPF offices to ensure that information is logged by an appropriate member of staff to ensure that accurate records are maintained and available on request (e.g. audit purposes).
- e) Similarly, once in receipt of information from a KMPF partner, it will be the responsibility of the KMPF Support Team to ensure that any information that is either awaiting processing or has been processed is stored in a secure location.

8. Information Storage

- 8.1 Student data is stored on the electronic **Higher Education Access Tracker (HEAT) database**, in accordance with the Data Protection Act 1998 and will be used only to administer and evaluate the project.
- 8.2 The HEAT database is held on secure computer systems which are subject to stringent physical and electronic access control mechanisms. A copy of the HEAT Data Protection Policy is available upon request by emailing kmpf@canterbury.ac.uk.
- 8.3 The HEAT database is password protected and different permission levels are set up to ensure only a small number of named database users have access to information at area administration level. KMPF has a list of all the users located in the Kent and Medway area who have access to information through the HEAT database and their permission level.

- 8.4 All new and existing KMPF staff who have access to information relating to the project will be made aware of the conditions of this policy and sign a confidentiality agreement with KMPF which will be kept on file.
- 8.5 KMPF Partners will add to participant information and activities on the HEAT database but must not change or delete student records or activities without discussion with the KMPF Support Team.

9. The distribution of information to third parties

- 9.1 Students' personal information will not be disclosed unless absolutely necessary and only for the purposes of monitoring and evaluating the programme or where there is a clear legal requirement to provide information. Student information will not be shared with anyone who is unauthorised.
- 9.2 KMPF participant details will be shared with the **HEAT service** (see Section 8), hosted by the University of Kent, for the purposes of **storage, data monitoring and evaluation**. An information sharing agreement is in place between KMPF and HEAT for this purpose (available upon request by emailing kmpf@canterbury.ac.uk).
- 9.3 For **research and monitoring purposes only**, KMPF participant details may also be shared with colleagues and educational partners involved in KMPF, including the **Office for Students (OfS), the Department for Education (DfE), the Higher Education Statistics Agency (HESA), the University and Colleges Admissions Service (UCAS)**, our partners (including **colleges, HEAT subscribers, and the Education and Skills Funding Agency**) and other educational services organisations with whom we have an information sharing agreement (listed on our website at www.kmpf.org). This will enable us to evaluate the effectiveness of this activity as part of the government policy to widen participation in higher education and to develop future policy.
- 9.4 We will ask school partners to obtain appropriate consent for collecting and sharing students' personal information (see Section 5). Parents and students can opt out of student data recording and data sharing at any time by contacting kmpf@canterbury.ac.uk.
- 9.5 Data will not be shared outside of the European Economic Area (EEA).

10. The disposal of information

- 10.1 Information kept in paper form will be destroyed one year after the information has been electronically recorded. The paperwork must either be shredded or arrangements made for a special collection by Canterbury Christ Church University by those responsible for the safe destruction of confidential waste. Records of destruction are kept by Canterbury Christ Church University.
- 10.2 Data stored electronically will only be deleted once approval has been sought from the KMPF Supervisory Directorate.
- 10.3 Data stored on the HEAT database will be securely deleted once it is no longer required for the purposes of the project. A data retention schedule for HEAT is available upon request by emailing kmpf@canterbury.ac.uk.
- 10.4 The KMPF Support Team will retain a written summary of the data destroyed either physically or electronically. The summary will contain details of data type e.g. questionnaire, baseline student data, the data held within it e.g. date of birth, home address, the time period the data refers to and the quantity. The summary will be produced on request by appropriate bodies (e.g. funding councils).

11. Data requests

- 11.1 Under the Data Protection Act 1998 participants have the right to a copy of the data held about them by KMPF. If an individual or a school has any concerns about the use of data for the purposes described in this policy, or would like a copy of the data that they have supplied directly to KMPF, these requests should be made by emailing kmpf@canterbury.ac.uk.

12. Review

- 12.1 This policy will be reviewed annually in conjunction with KMPF partners and the Data Protection Officer for Canterbury Christ Church University as hosting organisation for KMPF.