

## **Data Protection Policy**

### **Introduction**

Feligrace Limited needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and comply with regulations and legislation. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Feligrace must comply with the Data Protection Principles set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

Feligrace and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure this happens, Feligrace has developed this Data Protection Policy. It is important that everyone at all levels across Feligrace is familiar with the Data Protection Policy and understands their role and responsibilities. Noncompliance with any part of the Data Protection Policy will be a breach of Feligrace's policies and procedures and may result in disciplinary action, including dismissal in respect of staff and expulsion in respect of students. Potential breaches may include, but are not limited to, those noted within each section of this policy. Feligrace promotes respect, fairness and courtesy within the workplace and views the potential harassment or bullying of an individual as a very serious matter. Claims of potential harassment or bullying through technology provided by Feligrace will not be tolerated and will be investigated and dealt with in line with the disciplinary policies and procedures of Feligrace. Users should ensure that any message sent via email, collaborative applications or any other form of technology could not be misconstrued or contain language or tone that may cause offence.

### **Status of the policy**

This policy in keeping with other college policies does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by Feligrace from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings. Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with a designated data

controller initially. If the matter is not resolved it should be raised as a formal grievance. This will be referred to the Director for a final hearing should it continue to be unresolved.

## **Notification of Data Held and Processed**

All staff, students and other users are entitled to

- Know what information Feligrace holds and processes about them and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what Feligrace is doing to comply with its obligations under the 1998 Act.

Feligrace will therefore provide all staff and students and other relevant users with a standard form of notification on request. This will state all the types of data Feligrace holds and processes about them, and the reasons for which it is processed.

## **Responsibilities of all the Users**

Feligrace equipment and systems, including all telephone and computer facilities, including college Wi-Fi whether accessed from Feligrace or via external lines, home or mobile connection, are a college tool and are provided for Feligrace use. The principle of acceptable use is to avoid systems being misused, to minimise the potential for security breaches and/or loss of data to ensure all systems are used to maximum college benefit. It is Feligrace's aim to protect systems from inappropriate usage through a combination of policy, technological controls and monitoring. Inappropriate usage could put Feligrace's data at risk and expose Feligrace to legal liabilities.

Further guidance is contained within related Internet Email & Computer Policy. Staff should refer to the Staff e-safety and Acceptable Use Policy, Social Media Policy, and Mobile Devices Policy and students should refer to the Student IT Acceptable Use Policy.

The following materials must not be downloaded, distributed, viewed, copied, printed or disseminated onto or via Feligrace equipment and systems or own devices:

- Obscene, pornographic or sexually explicit material.
- Information and materials regarding terrorism or cults.
- Information and materials regarding online dating.
- Information and materials regarding controlled drugs for criminal purposes.
- Information and extreme material which may be likely to cause offence to another person.
- Information and materials regarding "hate sites" (racial or other) conducting political activity.
- Information and materials regarding gambling.
- Information and materials regarding criminal "skills" (including software hacking).
- Information and materials regarding chat sites or on-line discussion sites (including client based or web based Instant Messaging services).
- Information and materials regarding chain mail or jokes which others may find offensive.
- Information and materials regarding internet broadcasts (unless such a broadcast needs to be received for business purposes) or other internet media (such as YouTube).
- Information regarding images, cartoons and games.

Where information and materials contained in the above list are essential for teaching and learning or academic research or intended for promoting staff and student well being (such as sexual health information) it will be permissible to access them. For the avoidance of doubt, staff should contact the Director to clarify acceptable use.

Personal use of Feligrace systems, including e-mail and the Internet, is allowed so long as usage:

- Is kept to a minimum, normally outside Feligrace normal working hours and does not interfere with work or the working environment,
- is not for any illegal activity or any activity which could bring Feligrace into disrepute or open Feligrace up to legal action, including the types of information listed above,
- Does not impact Feligrace's ability to provide either the e-mail system or Internet access for legitimate college purposes.

No software should be downloaded and/or installed onto any system unless permission is given via the concerned department. This specifically includes software which is intended to be used with a web browser, often known as a 'plug-in', (e.g. toolbars). Only USB mass storage or other similar devices that are provided by Feligrace should be used.

Staff and students often participate in social networking sites including but not limited to Facebook and/or Twitter either through Feligrace technology or outside normal college hours. It is important to note that any inappropriate communication via those sites that affects anyone associated with Feligrace, including but not limited to staff or students of Feligrace, may expose Feligrace to legal claims and/or bring Feligrace into disrepute. As indicated above, Feligrace promotes respect, fairness and courtesy within the workplace and views the potential harassment or bullying of anyone connected to Feligrace including but not limited to a member of staff, student, agency work or governor as a very serious matter. Users should ensure that any message sent via email, collaborative applications or any other form of technology could not be misconstrued or contain language or tone that may cause offence. Claims of potential harassment or bullying via those forms of communication whether through Feligrace technology or not will not be tolerated and will be investigated and dealt with in line with the disciplinary policies and procedures of Feligrace. Any inappropriate communication in this way, if proven, may result in the summary dismissal of a member of staff and/or expulsion of a student.

## **Responsibilities of all the Users**

All staff is responsible for

- Checking that any information that they provide to Feligrace in connection with their employment is accurate and up to date.
- Informing Feligrace of any changes to information, which have been provided, i.e. changes of address
- Checking the information that Feligrace will send out from time to time, giving details of information kept and processed about staff.
- Informing Feligrace of any errors or changes. Feligrace cannot be held responsible for any errors unless the staff member has informed Feligrace of them.

If and when, as part of their responsibilities, staff collect information about other people, (i.e. about students course work, opinions about ability, references to other academic institutions, or details of personal circumstances). They must comply with the guidelines for staff, which are at appendix A.

## **Bring your own Device**

The use in the workplace by staff of non-college owned electronic devices such as smart phones, tablets and other such devices to access and store college information, as well as their own is commonly known as 'bring your own device' or BYOD. As data controller Feligrace must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. As an employee you are required to keep secure college information and data. This applies equally to information held on the college systems and to information held on an employee's own device.

As an employee you are required to assist and support the college in carrying out its legal and operational obligations with regard to college data and information stored on your device. This includes security of transfer of data between the personal device and the college system. You are required to cooperate with officers of the college when they consider it necessary to access or inspect college data stored on your device.

Where a staff member uses their own device to access and store data that relates to Feligrace then it is their responsibility to familiarise themselves with the device sufficiently in order to keep the data secure. In practice this means:

- Preventing theft and loss of data,
- where appropriate keeping information confidential and
- maintaining the integrity of data and information.

You should:

- Delete sensitive or commercial emails once you have finished with them
- Delete copies of attachments to emails such as spread sheets and data sets on mobile devices as soon as you have finished with them
- Limit the number of emails and other information that you are syncing to your device.

In the event of a loss or theft, you should change the password to all college services accessed from the devices (and it is recommended this is done for any other services that have been accessed via that device, e.g. social networking sites, online banks, online shops).

In event of loss or theft of a device you should report the matter promptly to the IT Helpdesk to enable access to college systems by a device or user to be revoked and/or the activation of a remote locate and wipe facility operated by the college. It is recognised that remote wiping of data may result in the loss of the employee's personal information held on the device.

## **Data Security**

All staff is responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be

- Kept in a locked filing cabinet; or
- In a locked drawer; or
- If it is computerised, be password protected; or
- Kept only on disk which is itself kept securely.

Staff should take care to log out of their PC when they are away from their workstation and keep their desk clear of personal data when away from their desk and keep personal information in a locked filing cabinet or locked drawer.

## **Student Obligation**

Students must ensure that all personal data provided to Feligrace is accurate and up to date. They must ensure that changes of address, etc are notified to their tutor co-ordinator or other departmental administrator for onward transmission to the Threshold Team.

## **Right to Access Information**

Staff, students and other users of Feligrace have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the college "Access to information" form and give it to the data controller/their personal tutor.

In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing using the standard form attached, appendix B.

Feligrace will not normally make a charge on each occasion that access is requested. However should excessive or vexatious requests be received Feligrace will make a charge of £5 per request.

Feligrace aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 21 days unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

## **Publication of Feligrace Information**

Information that is already in the public domain is exempt from the 1998 Act. The following information will be available to the public for inspection:

- Names and contacts of college governors
- List of staff
- Photographs of key staff

Feligrace internal telephone list will not be a public document. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the designated data controller.

## **Subject Consent**

In many cases, Feligrace can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to Feligrace processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.

Feligrace will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. Feligrace will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

Therefore, all prospective staff and students will be asked to sign a Consent To Process form, regarding particular types of information when an offer of employment or a course place is made. A refusal to sign such a form can result in the offer being withdrawn.

## **Processing Sensitive Information**

Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure Feligrace is a safe place for everyone, or to operate other college policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, Staff and students will be asked to give express consent for the Feligrace to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the designated data controller.

Feligrace as a body corporate is the data controller under the Act, and the Corporation is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day to day matters.

Designated data controllers include the following staff:

Director

Admissions Manager

Information Services Compliance Officer

## **Retention of Data**

Feligrace will keep some forms of information for longer than others. Because of storage problems, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general information about students will be kept for a maximum of five years after they leave Feligrace. This will include

Name and address,

Academic achievements, including marks for coursework

Disciplinary matters and academic appeals and

Copies of any reference written

All other information, including any information about health, race will be destroyed within 3 years of the course ending and the student leaving Feligrace.

Feligrace will need to keep information about staff for longer periods of time. In general, all information will be kept for five years after a member of staff leaves the college. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, and information required for job references. A full list of information with retention times is available from the data controller, appendix C.

## **Conclusion**

Compliance with the 1998 Act is the responsibility of all members of Feligrace. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to Feligrace facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of the policy should be taken up with the designated data controller.

## APPENDIX A:

### Staff Guidelines for Data Protection.

1. All staff will process data about students on a regular basis, marking registers, writing reports or academic references, or as part of pastoral or academic supervision. Feligrace will ensure that through registration procedures all students give their consent to this sort of processing and are notified of the categories of processing as required by the 1998 Act. The information that staff deal with on a day to day basis will be “standard” and will cover categories such as:
  - General personal details such as name and address,
  - Details of attendance, course work marks and grades and associated comments.
  - Notes of personal supervision, including matters about behaviour and discipline.
  
2. Information about a student’s physical or mental health: sexual life: political or religious views: trade union membership or ethnicity or race is sensitive and can only be collected and processed with the students consent. If staff needs to record this information, they should use a standard college form.  
e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.
  
3. All staff has a duty to make sure they comply with the data protection principles, which are set out in the Data Protection Policy. In particular staff must ensure that records are :
  - Accurate;
  - Up to date;
  - Fair;
  - Kept and disposed of safely and in accordance with the policy.
  
4. Feligrace will designate selected staff as “authorised staff”. This staff is the only staff authorised to hold or process data that is:
  - Non standard data; or
  - Sensitive data.The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is urgent and necessary in all the circumstances. E.g. a student is injured and unconscious but in need of medical attention and a staff member tells the hospital that the student is pregnant.
  
5. Authorised staff will be responsible for ensuring that all data is kept securely.
  
6. Staff must not disclose personal data to any student, unless for normal academic or pastoral purposes, without authorisation or agreement from the data controller, or in line with the data protection policy.
  
7. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement of the designated data controller, or in line with the policy.



8. Before processing any personal data, all staff should consider the following checklist:

- Do you really need to record the information?
- Is the information “standard” or is it “sensitive”?
- If it is sensitive, do you have the data subject’s express consent?
- Has the student been told this type of data will be processed?
- Are you authorised to collect/store/process the data?
- If yes have you checked with the data subject that the data is accurate?
- Are you sure that the data is secure?
- If you do not have the subject’s consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?
- Have you reported the fact of data collection to the authorised person within the required time?

## APPENDIX B:

### Standard form to request Access to Data:

I \_\_\_\_\_ wish to have access to either [delete as appropriate]

1. All the data that Feligrace currently has about me, either as part of an automated system or part of a relevant filing system; or
2. Data that Feligrace has about me in the following categories:
  - Academic marks or coursework details
  - Academic or employment references
  - Disciplinary records
  - Health and Medical matters
  - Political, religious or trade union information
  - Any statements of opinion about my abilities or performance
  - Personal details including name, address, date of birth etc.
  - Other information

[Please tick as appropriate]

I understand that I will have to pay a fee of £.....

Signed.....

Dated.....

## APPENDIX C:

How Feligrace Limited and Adult Education uses Personal Information. The General Data protection Regulation (or GDPR for short) is a positive step towards you having more control over how your data is used. Feligrace Limited is committed to clearly explaining what data we collect, its purpose, how long we keep it for and who we would share it with. The table below identifies this.

Data we collect	Why we collect it	Who we share it with	How long we keep it for
Sensitive Data such as Name, Address, Date of Birth, Contact details, Ethnicity, National Insurance Number, Gender, Learning Difficulty, Disability	We collect this data on behalf of our Funding Bodies. For more details about how they use your data please visit their <a href="https://www.gov.uk/government/publications/learning-records-service-the-plr-for-learners-and-parents">website</a> <a href="https://www.gov.uk/government/publications/learning-records-service-the-plr-for-learners-and-parents">https://www.gov.uk/government/publications/learning-records-service-the-plr-for-learners-and-parents</a>	The Education and Skills Funding Agency and the Department for Education	Until 2030 for accredited learning 7 years from completion for non-accredited learning
As Above	Register learners for qualifications	Awarding bodies - various	As above
As Above	Report safeguarding concerns to the Safeguarding Board	Safeguarding Board	Up to the learner's 25th birthday
As Above	IT Account creation	Google sites	+ 1 year post qualification achievement /end of course
As Above	IT Account creation	E Portfolio	+ 6 years post qualification
As Above	Follow up post course to see what impact the training has had	External company for learner destination	Report will be retained as per the funding data. The company will retain the data for the duration of the contact
As Above + parental contact and Doctor contact		Crèche registration	+ 2 year from last visit
As Above		Additional Learning Needs/ Education Health Care Plan	As per funding data

If you have any questions about Data Protection and Feligrace Limited, please contact:

[info@feligrace.com](mailto:info@feligrace.com)

Feligrace Limited  
Unit 11, 33 River Road Business Park  
River Road  
Barking  
IG11 0EA

## APPENDIX D:

### Website Privacy Policy

#### Introduction

Companies that gather personal data have to, by law, notify the Information Commissioner that they are doing so. At Feligrace we are totally committed to protecting your personal information and will look after the information you entrust to us keeping it safe and secure. Feligrace complies with this requirement, and its Data Protection Registration No. is Z217877X

#### Principles of Data Protection

Anyone processing personal data must comply with the eight enforceable principles of good practice. The Data Protection Act 1998 states that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure;
- not transferred to countries without adequate protection.

Personal data covers both facts and opinions about the individual. It also includes information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'.

The full explanation of the principles can be found here <http://www.ico.gov.uk>

The sections below explain the Feligrace privacy policy.

1. Statement of intent
2. Information on users
3. Disclosing Personal Information
4. Access to your Personal Information
5. Direct Marketing
6. Users under 18 years

## **Statement of intent**

From time to time, you may be asked to submit personal information about yourself (e.g. name, email address etc) in order to receive or use services on our web site. By entering your details in the form fields requested, Feligrace will be able to provide you with the services you choose and provide you with the information you wish to receive. Whenever you provide such personal information, we will treat that information in accordance with the Data Protection Act 1998 and will not in any event share or disclose your data with any other third party without first obtaining your consent. Feligrace will act in accordance with current UK legislation and aim to meet current Internet best practice. Advice from the Legal Service will be sought to keep this Policy up to date.

## **Disclosing Personal Information**

When you supply any personal information to Feligrace we have legal obligations towards you in the way we handle that data. We have to collect the information fairly, and to let you know how we will use it and whether we will pass the information on to anyone else. We will hold your personal information on our systems for as long as you use the service you have requested, and remove it in the event that the purpose has been met. We will ensure that all personal information supplied is held securely, in accordance with the Data Protection Act 1998.

## **Access to your Personal Information**

You have the right to access and correct your personal information and privacy preferences. This may be accomplished by writing to Feligrace at:

[info@feligrace.com](mailto:info@feligrace.com)

Feligrace Limited  
Unit 11, 33 River Road Business Park  
River Road  
Barking  
IG11 0EA