The Family Forge Data Protection Policy 2018
Review date: December 2018

Compiled The Family Forge/Jocelyn Owens – Controller/ Data Protection Officer

The Family Forge
4 Cobbs Brow Lane
Newburgh
Lancs
WN87ND
info@familyforge.org

Contents

1.The Current Legislation – the GDPR – General Data Protection Regulation
2.The Family Forge Data protection Policy – p 8
3. The Family Forge Privacy Notice -p9

The Current Legislation- The GDPR

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It has been adopted by the UK and will not be affected by Brexit negotiations and will apply in the UK from May 2018.

What is personal data under GDPR?
"**Personal data**" means any information relating to an identifiable person. An identifiable person is one who can be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location and so on.

What is considered sensitive personal data?

The Act provides a separate definition for "**sensitive personal data**". This relates to information concerning a **data** subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, sexual life, or details of criminal offences.

Is a name and address personal data?
By itself the **name** John Smith may not always be **personal data** because there are many individuals with that **name**. However, where the **name** is combined with other information such as an **address**, a place of work, or a telephone number this will usually be sufficient to clearly identify one individual and as such becomes personal data.

What is the definition of data protection?
Data protection is commonly defined as the law designed to **protect** your personal information, which is collected, processed and stored by "automated" means or intended to be part of a filing system.

What is the data controller?

The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal **data** are, or are to be, processed.

A **Processor** acts on the controller's behalf to obtain, record or hold information.

The GDPR places specific legal obligations on processors; for example, processors are required to maintain records of personal data and processing activities.

For processing to be lawful under the GDPR, processors must identify a lawful basis before they can process personal data.

Consent under the GDPR must be a freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be some form of a clear positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions needed, and simple ways for people to withdraw consent must be provided..

For consent to meet the requirement of the GDPR, consent must be specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn.

Children's personal data

The GDPR contains new provisions intended to enhance the protection of children's personal data.

Privacy notices for children

Where services are offered directly to a child, privacy notices must be written in a clear, plain way that a child can understand.

Online services offered to children

If online services are offered to children consent from from a parent or guardian to process the child's data may be required.

The GDPR states that, if consent is your basis for processing the child's personal data, a child under the age of 16 can't give that consent themselves and instead consent is required from a person holding 'parental responsibility' – but note that it does permit member states to provide for a lower age in law, as long as it is not below 13.

'Information society services' (online services) includes most internet services provided at the user's request, normally for remuneration. The GDPR emphasises that protection is particularly significant where children's personal information is used for the purposes of marketing and creating online profiles.

Parental/guardian consent is not required where the processing is related to preventative or counselling services offered directly to a child.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification

4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The right to be informed obliges the processor to provide 'fair processing information'. This is usually done through a **privacy notice**. It emphasises the need for transparency over how personal data is used.

Privacy notices must be

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The Privacy notice must include

- the name of the Controller of the Data (The Family Forge in our case) along with contact details, the identity and contact details of any representatives acting for the Controller and the Data Protection Officer's identity and contact details.
- The purpose and lawful basis of the processing of this information
- The legitimate interests of the third parties if applicable
- categories of personal data being collected
- any recipients of the personal data
- details of any transfers of the data to third parties and safeguards
- the retention period of the data or the criteria used to determine the retention period of the data.
- The existence of the data subjects rights
- the right to withdraw consent at any time
- the right to lodge a complaint with the supervisory authority
- the source the personal data originates from and whether it came from publicly accessible sources
- whether the provision of personal data is part of a statutory requirement or contractual obligation and the consequences of failing to provide such personal data
- the existence of automated decision making if there is any using the data provided, including profiling and how decisions are made, the significance and the consequences of it.

This information should be provided at the time the data is obtained or at the very least before it is disclosed to another recipient if a disclosure is envisaged. Anyhow within one month of receiving the data.

Right to access the information If the information held is requested by the subject of the information, it must be provided free, without delay and at least within one month of the request after having verified the identity of the subject requesting the information by reasonable means.

Right to Rectification Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. This rectification must be passed on to third parties if applicable when their information is also inaccurate where possible and the subject informed re the third parties that have received the information.

Individuals have a right to erasure. This is the right to be forgotten. This means that an individual has the right to the removal or deletion of personal data where there is no compelling reason for its continued processing.

The right to be forgotten is not an absolute right but applies where:
•the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
•When the individual withdraws 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 (ie otherwise in breach of the GDPR).
•The personal data has 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 to a child.

The right to restrict processing

Restriction of the processing of data is required in the following circumstances:
•Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.
•Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.
•When processing is unlawful and the individual opposes erasure and requests restriction instead.
•If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

The right to Data portability
The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The Right to object

If you process personal data for the performance of a legal task or your organisation's legitimate interests individuals must have an objection based on "grounds relating to his or her particular situation".

In this case the processor must stop processing the personal data unless:
•it can be demonstrated that there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
•the processing is for the establishment, exercise or defence of legal claims.

The legal requirement is to inform individuals of their right to object "at the point of first communication" and in your privacy notice.
This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

Processing for direct marketing purposes
Processing personal data for direct marketing purposes mus t be stopped as soon as an objection is received. The law states that there are no exemptions or grounds to refuse.
Objection must be dealt with at any time and free of charge.
Individuals must be informed of their right to object "at the point of first communication" and in the privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".
These requirements are similar to existing rules under the DPA.

Rights in relation to automated decision making and profiling.

In brief…
The GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention.
Data protection by design and by default.
The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements.
Organisations are required to put into place comprehensive but proportionate governance measures. Good practice such as privacy impact assessments and privacy by design are now legally required in certain circumstances.
The accountability principle?
The new accountability principle in Article 5(2) requires that it be demonstrated that we comply with the principles of accountability and state explicitly that accountability is our responsibility.

To demonstrate compliance
The following must be done if appropriate for data collection that is carried out:
•Implement appropriate technical and organisational measures that ensure and demonstrate compliance.
•This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
•Maintain relevant documentation on processing activities.
•Where appropriate, appoint a data protection officer.
•Implement measures that meet the principles of data protection by design and data protection by default.
Measures could include
•Data minimisation;
•Pseudonymisation;
•Transparency;
•Allowing individuals to monitor processing; and
•Creating and improving security features on an ongoing basis.
•Use data protection impact assessments where appropriate.

Data protection impact assessment?

Data protection impact assessments (DPIAs) (also known as privacy impact assessments or PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.
See the ICO's Conducting privacy impact assessments code of practic efor good practice advice.

You must carry out a DPIA when:

•using new technologies; and
•the processing is likely to result in a high risk to the rights and freedoms of individuals.

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Data Protection Officers

Under the GDPR, a data protection officer (DPO) must be appointed if you:

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR.
A Data Protection Officer must be appointed if you are:

1. a public authority (except for courts acting in their judicial capacity)
2. carry out large scale systematic monitoring of individuals (for example, online behaviour tracking); or
3. carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

You may appoint a single data protection officer to act for a group of companies or for a group of public authorities, taking into account their structure and size.

D**ata protection officer qualifications**

The GDPR does not specify the precise credentials a data protection officer is expected to have.
It does require that they should have professional experience and knowledge of data protection law. This should be proportionate to the type of processing your organisation carries out, taking into consideration the level of protection the personal data requires.

Breaches of Data Protection

The GDPR is introducing a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected.

What is a personal data breach?
A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.
What breaches are required to be notified to the relevant supervisory authority ?
You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.
This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach **leaves individuals open to identity theft**. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

When do individuals have to be notified?
Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.
A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.
A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it. The GDPR recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases.
If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.
Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover.

Preparation for breach reporting?
The law requires **making sure that staff understands what constitutes a data breach**, and that this is more than a loss of personal data.
I**nternal breach reporting procedure is required.** This will facilitate decision-making about whether you need to notify the relevant supervisory authority or the public.
In light of the tight timescales for reporting a breach - it is important to have robust breach detection, investigation and internal reporting procedures in place.

Transfers of personal data outside the EU.
The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations. A transfer, or set of transfers, may be made where the transfer is:
•made with the individual's informed consent;
•necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.
What about one-off (or infrequent) transfers of personal data concerning only relatively few individuals?
Even where there is no Commission decision authorising transfers to the country in question, if it is not possible to demonstrate that individual's rights are protected by adequate safeguards and none of the derogations apply, the GDPR provides that personal data may still be transferred outside the EU.

The Family Forge Data Protection Policy

1. Permission will required on registration at the Family Forge from the data subject to allow the Family Forge to hold personal data

2. Parental permission must be obtained to register and keep any personal information from minors (under 16 for data protection regulations). The name of the parent giving permission must be noted.

3. For online services in particular an option to withdraw consent from holding personal data must be provided so that permission may be withdrawn at any time. This should also apply to manual forms by making this clear in privacy notices.

4. Manual filing systems containing personal data shall be kept in lockable filing cabinets. Trustees are to keep secure any files containing personal data in their care off site. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data at all times, including the preventing of unauthorised access to or use of the personal data or the equipment used for processing it.

5. Contact lists and attendance data shall be password protected.

6. If data is passed to a third party it shall be sent as an attachment to our partners and only to the person requiring the data on a need to know basis and never sent in the main email itself.

7. All personal data held on the computers or manual filing systems shall be reviewed annually and deleted where class attendance or other forms of contact have ceased for periods longer than 6 months to one year as appropriate.

8. Details contained on mobile phone shall be removed by tutors 4 months after the last lesson was attended by any individual student.

9. Attendance details shall be kept for no longer than 5 years.

10. Whenever a new technology is introduced the Family Forge will undertake a data protection impact assessment according to the guidelines of the GDPR.

11. All staff will notify the Data Protection Officer of data breaches and be made aware of what constitutes a notifiable data breach to the relevant authorities.

12. The Data Protection Officer will report any serious breach of Data Protection to the relevant authorities within 72 hours of the breach and in some cases to the individuals concerned, if the breach is likely to result in a risk to the rights and freedoms of individuals for example discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

An example of this might be where the breach leaves individuals open to identity theft. The simple loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

13. **Failure to report a breach may result in a substantial fine.**

14. **Where a breach is likely to result in a high risk to the rights and freedoms of individuals, The Family Forge Data Protection Officer will notify those concerned directly.**

15. **Staff must inform the Data Protection Officer of any breach that they are aware of that may damage the rights and freedoms of any individual. To do this they will write a report containing the following information.**

- **The nature of the personal data breach including, where possible:**
- •the categories and approximate number of individuals concerned; and
- •the categories and approximate number of personal data records concerned;
- •The name and contact details of the data protection officer or the name of the contact point where more information can be obtained including the name of the member of staff making the report;
- •A description of the likely consequences of the personal data breach;and
- **•A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects**

16. **All staff will be given a copy of the Data Protection Policy of the Family Forge and made aware of their obligations under the GDPR legislation.**

The Family Forge Privacy Notice

I give my consent to the Family Forge to use my data according to this privacy notice. I have been informed that I may withdraw my consent at any time by verbal communication or other form of text or written notice.

Signed …..... Date.....

I would like to Unsubscribe …..

The Controller/ processors and Data Protection Officer

The Family Forge is the controller for data collection purposes directing the purposes and the means by which your personal data is processed for the charity and its services. The Data Protection Officer is Jocelyn Owens Trustee/ Manager at the Family Forge. Contact details: 4 Cobbs Brow Lane, Newburgh. WN8 7ND Tel. 01257 464813 or mobile 07947 853 502.

The processors of the information are the management and tutors at the Family Forge and also paypal/credit card companies for the processing of online payments. General website statistics are collated by our website host- G- suite. Currently we also use the services of Wiziq for the booking of some online tutoring. Please see the privacy notice of Wiziq if you use this service as it is not under our control.

Tutors are Elizabeth Quispe -contact via info@familyforge.org and Paula Walsh contact via info@familyforge.org.
Trustees are Michael Turner and Esperanza Arenas Arguelles

The Family Forge recognises that the the protection of personal data covers both technological collection of data and manual systems. The Family Forge endeavours to comply with the current legislation on Data protection in order to keep your personal data secure.

The Legal Basis for collecting Data

The Legal basis of the Family Forge to process some personal data falls under GDPR May 2018 section

6(1)(f) – Legitimate Interests
The Family Forge collects certain data as it is necessary to carry out our legitimate interests namely our charitable services or online teaching. But we recognise that we are subject to the interests, rights or freedoms of the data subject. Specifically charities that provide funding may also require basic personal data- this applies to staff/ trustees/ tutors/ and volunteers or specific people who are being funded to receive certain services.

And
6(1)(a) – Consent of the data subject.
In other words the Family Forge asks for personal data and only acts on the consent of the data subject – that is the people either using the Family Forge services/ the staff/volunteers or supporters for the purposes of offering those services or in order to provide the means to support the organisation in other ways including through fundraising, marketing or the passing of information which may be of interest to them.

And also
9(2)(b) – the Family Forge must process certain information in order to carry out obligations under employment, social security or social protection law, or a collective agreement. (e.g DBS applications, regulatory requirements for bodies such as Ofsted or other partners such as schools).

The Information we collect

The Family Forge collects some or all of the following information about you based on whether you are a student/refugee/online student / subscriber for fundraising or marketing purposes /volunteer/tutor or trustee or other user of the Family forge Life Skills Centre:

Name
Address
Mobile or Home Telephone number- the most appropriate for communicating
Email address
Nationality and Mother tongue and other languages spoken
Marital status
Numbers of Children
Religion
Date of Birth
Citizenship Status
Educational Background

Employment background
Other skills or hobbies
Personal allergies or illness
Class/talk or course attendance records
Class attainment records and assessment recordings
Records of Payments received (if any)
Website usage statistics
Permissions for photo usage given

In addition to this The Family Forge may collect the following information about its' staff or volunteers:
Disclosure and Barring Service reports and Numbers
References

For funding bodies or individual donors we also keep records of donations or grants received and records of appeals responded to.

Occasionally we may use information collected from publicly accessible sources for fundraising purposes.

Why we collect Personal Data

The data is collected in order that the Family Forge can provide a tailored service to its users helping to identify the needs and progress of students and is useful in marketing and fundraising. It also provides accountability for regulatory bodies so that our legal obligations can be fulfilled and safeguarding and health and safety requirements be adhered to.
Whilst for the majority of our data subjects there are few consequences of not holding their personal data, for some (volunteers/ trustees and Staff) it would result in our inability to comply with certain regulatory requirements e.g. DBS status of volunteers. Other regulatory bodies may also require attendance records to be kept.

The Family Forge does not engage in automated decision making.

The recipients of the personal data collected by the Family Forge are the

tutors, the manager, the trustees (all listed above) and occasionally funding bodies, school partners or official bodies such as Ofsted or the Disclosure and Barring service. Personal data is only passed to these third parties for the carrying out of legitimate checks. It is the policy of the Family Forge where electronic methods are used to pass such information as an attachment and not in the main mail itself so that only the recipient can read the document. Once passed to a third party the third party becomes responsible for the data but we will send corrections to the data if required to do so. If you are concerned about third parties please ask to ascertain whether your specific information may be sent. Largely this applies where we work with partner organisations and not to activities solely organised by the Family Forge.

Contact details for adult students and colleagues are kept on the tutors mobile phones for the purposes of class reminder services. At no time are contact numbers for minors kept on tutors phones . This is a safeguarding requirement.
Contact details for students/ supporters are reviewed annually for both manual and computer filing systems and where class attendance or other forms of contact have ceased for longer than 6 months to 1 year, the contact details are removed. Contact details contained on mobile phones are removed by 4 months after the last lesson attended. Payment details are kept for up to 7 years in line with Tax Law and attendance details also.

Your Rights

Any person whose personal data we hold, has the right to request freely what data we hold and for it to be provided without delay, within at most one month of the data being requested after an identity check verifying the subject requesting the information is made. Also any person whose personal data we hold has the right to :

- rectification of any data that is incorrect.
- Erasure of data where there is no compelling reason for it to continue to be held that is the right to be forgotten although this is not an absolute right. See GDPR 2018
- the right to the restriction of processing subject to GDPR 2018
- the right to the portability or the reuse of their personal data subject to GDPR 2018
- the right to safeguarding against the risk that a potentially damaging decision is taken without human intervention based on profiling
- the right to object to data holding on the grounds of their particular situation again subject to GDPR 2018

Special note
When we use your data for direct marketing/fundraising purposes you have a right to object at any point and have the process stopped as soon as we receive your objection free of any charge. You also have the right to lodge a complaint with the appropriate supervisory authority.