Free Representation Unit – Data protection policy

Scope of policy

This policy applies to:

- Employees
- Casual staff
- Volunteers
- Management committee members and trustees
- All contractors, suppliers and other people working on behalf of FRU

Key policy details

Prepared by: Chief Executive, March 2016

Approved by: Management Committee
Operational date: October 2016
Review date: October 2017

Registration

FRU is registered as a data controller with the Information Commissioner's Office (ICO):
Registration number = ZA031976
Expiry date = 06/01/2018

Purpose of policy

The purpose of this policy is to ensure that Free Representation Unit (FRU):

- complies with the law in respect of the data it holds about individuals;
- follows good practice;
- protects FRU's clients, volunteers, supporters, staff and other individuals
- protects the organisation from the consequences of a breach of its responsibilities.

Data protection law and principles

The Data Protection Act 1998 describes how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy statement

FRU will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for the management committee on its responsibilities and staff and volunteers who handle personal data

FRU recognises that its first priority under the Data Protection Act is to avoid causing harm to individuals. In the main this means:

- keeping information securely in the right hands, and
- holding good quality information for no longer than necessary.

Secondly, the Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, FRU will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

FRU will never sell or give away data to anyone outside the organisation, unless compelled to do so by statute or an order of the court, or with the express consent of the individual.

Responsibilities

Everyone who works for or with FRU has some responsibility for ensuring data is collected, stored and handled appropriately. However, these people have key areas of responsibility:

- The trustees and management committee are ultimately responsible for ensuring that FRU meets its legal obligations.

- The Chief Executive, as data protection officer is responsible for:

    - Keeping the trustees and management committee updated about data protection responsibilities, risks and issues
    - Reviewing all data protection procedures and related policies
    - Arranging data protection training and advice for the people covered by this policy
    - Handling data protection questions from staff and anyone else covered by this policy
    - Checking and approving any contracts or agreements with third parties that may handle FRU's sensitive data
    - Approving any data protection statements attached to communications such as emails and letters
    - Ensuring that all new projects or initiatives comply with data protection principles

- The Office Manager is responsible for:

    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Ensuring security hardware and software is functioning properly
    - Evaluating any third-party services FRU is considering using to store or process data
    - Dealing with requests from individuals to see the data FRU holds about them ('subject access requests').

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Breaches of this policy will be handled under FRU's disciplinary procedures.

Communication with data subjects

FRU produces a privacy statement for data subjects, setting out how their information will be used. This will be available on request, and a version of this statement will also be used on the web site (see Appendix A). This policy will be published on the website.

Communication with staff and volunteers

Employees and casual staff will be required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities (see Appendix B).

The principles of this policy will form part of the volunteers guide and volunteers will be asked to agree to it at the point they sign up for a training day (see Appendix C).

Data accuracy

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary; staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated
- FRU will make it easy for data subjects to update the information FRU holds about them
- Data should be updated as inaccuracies are discovered eg, if a client or volunteer cannot be reached on their stored telephone number, it should be removed from the database.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Office Manager or Chief Executive. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet at FRU or an address known to and approved by FRU
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer
- Data printouts should be shredded and disposed of securely when no longer required
- When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts

Personal and sensitive data which is held electronically must be processed according to these guidelines:

- Data should be protected by strong passwords that are changed regularly and never shared between employees
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used
- Data should only be stored on designated drives and servers
- Servers containing personal data should be sited in a secure location, away from general office space
- Data should be backed up frequently and the backups should be tested regularly
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones unless the device has been encrypted

- All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to FRU unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees and volunteers should ensure the screens of their computers are always locked when left unattended
- Personal data should not be shared informally; in particular, it should never be sent by an email address not known to FRU
- If data is transferred electronically by a personally held electronic device, that device must be encrypted. Personal data should never be transferred outside of the European Economic Area
- Employees should not save copies of personal data to their own computers; always access and update the central copy of any data.

Retention periods

Data will be deleted or destroyed as follows:

- Employees – within seven years of leaving the organisation
- Casual staff – within seven years of leaving the organisation
- Clients – seven years after last contact
- Active Volunteers – at end of final client contact + seven years
- Non-Active Volunteers – within 15 months of attending training day
- Trustees and management committee – within seven years of leaving the organisation
- Supporters and donors – within three years of final contact

Data will be reviewed every 12 months and necessary steps will be taken to establish the relationship with the organisation of staff, MC members and trustees and volunteers.

Archiving

Archived paper client files are stored securely off site for six years.

Subject access requests

All individuals who are the subject of personal data held by FRU are entitled to:

- Ask what information is held about them and why
- Ask how to gain access to it
- Be informed how to keep it up to date.
- Be informed how FRU is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Any subject access requests will be handled by the Office Manager and reported to the Chief Executive.

Subject access requests must be in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Office Manager without delay.

All those making a subject access request will be asked to identify any volunteers or casual staff who may also hold information about them, so that this data can be retrieved.

The Office Manager will have regard to the Information Commissioner's Office 'Subject access code of practice' (http://ico.org.uk/for_organisations/data_protection/subject_access_requests) at all times when dealing with subject access requests.

Where the individual making a subject access request is not known to the Office Manager their identity will be verified before handing over any information.

The required information will be provided in permanent form unless the applicant makes a specific request to be given supervised access in person. FRU aims to respond to subject access requests within 28 days.

Transparency

FRU is committed to ensuring that in principle Data Subjects are aware that their data is being processed and

- for what purpose it is being processed
- what types of disclosure are likely
- how to exercise their rights in relation to the data

Data Subjects will generally be informed in the following ways:

- Staff: in the staff handbook
- Volunteers: in the volunteer guide
- Casual staff: in the staff handbook
- Clients: in the client care letter
- Trustees and management committee: by being given a copy of our policy
- Donors and supporters: when they sign up (on paper, on line or by phone) for services or purchase products

Further information

There are more detailed guides and data protection resources on the website of the Information Commissioner's Office (http://ico.org.uk/) and the Charity Finance Group produces a guide for charities – Protecting Data, Protecting People.

Appendix A: Privacy policy for users at [www.thefru.org.uk/privacy-policy]

This privacy policy sets out how Free Representation Unit uses and protects any information that you give Free Representation Unit when you use this website.
Free Representation Unit is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website, then you can be assured that it will only be used in accordance with this privacy statement.

Free Representation Unit may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from October 2016.

What we collect

We may collect the following information:

- name and job title
- contact information including email address
- demographic information such as postcode, preferences and interests
- other information relevant to customer surveys and/or offers

What we do with the information we gather

We require this information to understand your needs and provide you with a better service, and in particular for the following reasons:

- Internal record keeping.
- We may use the information to improve our products and services.
- We may periodically send promotional emails about new products, special offers or other information which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for market research purposes. We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your interests.

Security

We are committed to ensuring that your information is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect online.

Links to other websites

Our website may contain links to other websites of interest. However, once you have used these links to leave our site, you should note that we do not have any control over that other website. Therefore, we cannot be responsible for the protection and privacy of any information which you provide whilst visiting such sites and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

Controlling your personal information

You may choose to restrict the collection or use of your personal information in the following ways: whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes if you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by writing to or emailing us via the contact form on our website.

We will not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so. We may use your personal information to send you promotional information about third parties which we think you may find interesting if you tell us that you wish this to happen.

You may request details of personal information which we hold about you under the Data Protection Act 1998. A small fee will be payable. If you would like a copy of the information held on you please write to Free Representation Unit, Ground Floor, 60 Gray's Inn Road, London WC1X 8LU.

If you believe that any information we are holding on you is incorrect or incomplete, please write to or email us as soon as possible, at the above address. We will promptly correct any information found to be incorrect.

Appendix B: Confidentiality statement for staff and casual workers

When working for FRU, you will often need to have access to confidential information which may include, for example:

- Personal information about clients of FRU
- Personal information about FRU staff
- Personal information about individuals who are supporters or otherwise involved in activities organised by FRU.

FRU is committed to keeping this information confidential, in order to protect people and FRU itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must also be careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- Abide by FRU's file management procedure and not remove client files from the office without prior authorisation from a legal officer
- Not compromise or seek to evade security measures (including computer passwords);
- Not discuss confidential information with colleagues who do not need to know it or people outside FRU;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it;
- If you have to discuss confidential matters over the telephone make sure you cannot be overheard by anyone who does not need to have access the details being discussed;
- Make sure information on your computer, laptop, tablet cannot be accessed without your express permission. If you have to move away from your computer, laptop, tablet whilst working on a client case shut it down or lock it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with a FRU member of staff whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped working for FRU.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.

Signed: **Date:**

Print name:

Appendix C: Confidentiality statement for volunteers

When working for FRU, you will often need to have access to confidential information which may include, for example:

- Personal information about clients of FRU
- Personal information about FRU staff
- Personal information about individuals who are supporters or otherwise involved in activities organised by FRU.

FRU is committed to keeping this information confidential, in order to protect people and FRU itself. 'Confidential' means that all access to information must be on a need to know and properly authorised basis. You must use only the information you have been authorised to use, and for purposes that have been authorised. You should also be aware that under the Data Protection Act, unauthorised access to data about individuals is a criminal offence.

You must also be careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular you must:

- Abide by FRU's file management procedure and not remove client files from the office without prior authorisation from a legal officer
- Not compromise or seek to evade security measures (including computer passwords);
- Not discuss confidential information with colleagues who do not need to know it or people outside FRU;
- not disclose information — especially over the telephone — unless you are sure that you know who you are disclosing it to, and that they are authorised to have it;
- If you have to discuss confidential matters over the telephone make sure you cannot be overheard by anyone who does not need to have access the details being discussed;
- Make sure information on your computer, laptop, tablet cannot be accessed without your express permission. If you have to move away from your computer, laptop, tablet whilst working on a client case shut it down or lock it.

If you are in doubt about whether to disclose information or not, do not guess. Withhold the information while you check with a FRU member of staff whether the disclosure is appropriate.

Your confidentiality obligations continue to apply indefinitely after you have stopped volunteering for FRU.

I have read and understand the above statement. I accept my responsibilities regarding confidentiality.