Fire Officers' Association

DATA HANDLING AND COMMUNICATION POLICY

Approved by the Executive Board, May 2018

Contents

1. Introduction

Data Protection is taken seriously by the Fire Officers' Association and we constantly seek to improve our arrangements for dealing with members' personal information. This policy introduces revised procedures covering the Association's use and communication of information and data, particularly that relating to members' personal details.

We have considered the nature of data held and the magnitude of potential damage if it were lost or misused and conclude that we do not collect and process any more data than is necessary for running the Association, collecting subscriptions, communicating with members and for the provision of representation/advice in relation to employment matters.

However, much of the data held is sensitive and could be used to the disadvantage of members' if it were inappropriately released or misused. This document is, therefore, needed to set out conditions for the storage and use of membership information.

This policy document incorporates the Association's Privacy Notice as an Appendix to this document.

2. Purpose of the policy

The purpose of this document is:

- To set out why good information handling is important
- To draw attention to relevant legislation
- To set out the Association's policy in this area
- To set out procedures and checklists which will help top ensure that the policy is understood and implemented throughout the organisation.

3. Importance of effective and secure data handling

- Personal data must be safeguarded and handled safely and appropriately. If it falls into the wrong hands – deliberately or accidentally – or is misused, then financial and reputational loss to people and the organisation is a strong possibility.

- If data is used other than for purposes stated when obtained then personal annoyance and loss of trust in the organisation are very likely. Out of date information can lead to wrong decisions, wasted money and restricted access to membership services.

- Misuse of data is considered to be a disciplinary issue within the FOA and in may also be a criminal offence.

4. Personal data

Personal data is defined as any information about identifiable, living individuals which is:

- Held with the intention of entering into a computer or a relevant filing system
- Is on a computer or automated system
- In a relevant filing system (i.e. could be retrieved by someone looking for it)

It, therefore, includes any such information – names, photographs, email addresses, application forms, bank account details, computer records and many other examples. Anything that could identify, a living person is likely to be captured by this definition.

It does not include anonymised statistical or reference information (unless the sample is so small that the individuals concerned could be inferred from the statistical detail) or information about people who are no longer alive.

5. Relevant legislation

- Data Protection Act 1998
- Statutory instruments amplifying the Act
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Freedom of Information Act 2000
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation)

Enforcement is the responsibility of the Information Commissioner (www.ico.gov)

Data Protection statute requires that we observe certain principles, whilst allowing scope for interpretation and judgement. It is the Association's policy to observe good practice at all times.

This requires all staff and members to prevent harm by keeping data up to date and in the right hands, to build trust via openness about use of data, and to offer a choice about such matters where possible and appropriate.

The eight principles of Data Protection are that personal data must be: -

- fairly and lawfully processed
- processed for specified and lawful purposes and not in any manner incompatible with those purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not kept for longer than is necessary
- processed in line with the data subjects' rights
- secure
- not transferred to countries outside the European Economic Area without adequate protection

This policy sets out how the Fire Officers' Association will meet its obligations and observe these principles.

6. Data Protection Policy

a. Responsibilities

The Association as an organisation is the Data Controller and thus ultimately responsible for legal compliance.

The Chief Executive and the Trustees of the Association are responsible for ensuring that Data Protection policy is adequate, correct and reviewed regularly.

The Chief Executive, via the Association's Executive Board, is responsible for ensuring that procedures and training are in place to ensure that the Data Protection and Communication Policy is put into practice.

The Data Controller (this is the Association's Chief Executive) is responsible, for reviewing policy, preparing procedures, assisting on request with guidance and training, ensuring that the statutory notification is up to date and for reviewing contracts with external suppliers to ensure that the handling of personal data is adequate and well documented.

The term **Data Processor** refers to any member of staff or official who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve the processing of personal data.

Officials and staff members

Officials and Staff Dealing with Discipline, Grievance and Other Member Representation Matters

On completion of a case, that is, when any appeals, tribunals, ombudsman referrals or court cases have concluded, persons handling member representation cases must send (by secure means) all personal data relating to individuals (whether members or not) to Head Office for secure storage for a period of 6 years or until such time as the information is no longer necessary for legal or regulatory needs or to administer membership services,

Any copies of such case data or other material that may identify an individual must be destroyed or modified so as to make it anonymous.

Where any information pertaining to a case may be of use to the Association for reference or training purposes, identifying information will be removed or redacted before being made available for reference purposes.

All Officials and Staff Members

All officials and staff members are individually responsible for care in relation to these procedures, and for raising any queries, concerns or training needs which they might have.

On leaving any role within the Association, all records and data held by an official or staff member must be passed on to their successor or, in the absence of an identified successor, destroyed unless such material is unique in which case it should be sent to Head Office for safekeeping or disposal, as considered appropriate by the Chief or Assistant Chief Executive.

b. Confidentiality

All personal data and information encountered during Association work must be handled confidentially. Lists of personal data (including contact details and email addresses) may be passed to a third party only where agreed by the Chief Executive or the Executive Board. Staff likely to be involved in such transfers will be aware of appropriate procedures, which are documented below, and in case of doubt advice must always be sought.

A duty of confidentiality relating to Association work applies to members of staff, consultants and contractors and to Association members and associates carrying out Association work. Where appropriate, all Association members and staff taking part in meetings or project work will be asked to sign a pledge of confidentiality regarding the proceedings of the meeting or the conduct of the project.

Staff must not during or at any time after the termination (for whatever reason) of employment, disclose or use for their own benefit, any confidential information received or obtained in relation to the affairs of the Association. This includes but is not limited to member information, staff information, methods of data collection, patient information and records and all other research data.

Issues about colleagues or members of the Association must not be discussed outside of the Association in any situation where confidentiality would or could be compromised.

Information about the Association, colleagues or members must not be placed on any websites or social media unless authorised by the Association. Caution should be exercised when adding information to the Association website. The Chief Executive can advise where there is any doubt.

All notes, memoranda and other papers relating to the Association's business belong to the Association and must be handed over to the Association upon termination of employment or on leaving office (for whatever reason) and no copies shall be retained.

Confidentiality will only be over-ridden where it is required by law, for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty.

This policy does not affect protected disclosure i.e. "whistleblowing".

c. Security

The Association will take appropriate steps to protect data held on Association computers and other electronic storage media.

Data recording, storage and deletion

Data concerning members is held on a membership database and SAGE accounting software to which access is limited to Head Office staff and the Chief Executive. This information cannot be access via the Internet.

Specific permission must be sought from the Chief Executive before any other database is established. In this context, the term "database" includes for example, lists of names and addresses held electronically or on paper or email distribution lists held on Microsoft Outlook. It is recognised that there may be good reasons to hold such lists (provided they are updated regularly) but there is no presumption that they may be set up without specific permission.

Transparency in use of data

In collecting data the Association will always be transparent about the use to which they will be put. We ensure that our members, staff and contacts are aware of what we do by including the Data Protection statement (see appendices) every time we

collect data. The Association will explain and publicise its processes via information on the Association website and otherwise as may be useful from time to time.

Consent, opting in and opting out

On joining the Association and participating in its activities members must give explicit consent to certain uses of their data, as detailed in statements, privacy notices and Association policy.

In order to function as a Trade Union it is essential that certain information is passed to and used by third parties. In this context, this includes a solicitor, insurer or an organisation contracted to deliver services for the Association..

Subject access

There is a right of access to personal data (i.e. persons may request information about themselves). Any subject access request from a Member, Associate Member, member of staff, or from any other person should be directed to the Chief Executive or Assistant Chief Executive.

Applicants will be provided with the statutory permanent and intelligible copy of all personal data held about that data subject and the Association will respond within one month of receipt of a request.

d. Other

This policy will be reviewed as necessary and least annually.

A register will be kept of all instances of Association personal data handled by outside organisations, with relevant supporting documentation such as contracts and terms of business.

7. Procedures

The aim in setting out procedures which will implement the policies set out above is to ensure best possible practice.

The following procedures should be observed.

a. Requests from outside the Association for access to personal data

Association staff must not pass lists of contact data outside the Association. Queries received in writing from professional individuals or organisations, will be verified to confirm the source of the enquiry. If accepted, work contact details only will be supplied, unless the member in question has requested that this should not happen.

Requests from Association members for mailing lists or membership data for research or other activities should be referred to Head Office for consideration.

b. Use of laptops and electronic devices

All PCs containing key information will be protected by password protection.

Any sensitive information that needs to be communicated in electronic format should be password protected and /or encrypted.

Passwords must not be communicated by e-mail and should not be in the same communication as the protected material to which it applies.

c. Setting up new databases

Other than databases issued by the Association, any request to set up a new database must be approved by the Chief Executive. It is emphasised that the term "database" includes any recording of information electronically or on paper, and may be as simple as a list of names and email addresses.

d. Collecting data

Forms, whether paper or online, which collect personal data must always contain the Association's Privacy Notice.

e. Storing data

Confidential data (particularly bank or credit / debit card details) will be kept securely at Head Office and not left in open view when offices are unattended.

This provision applies to any other location where confidential data may be held.

f. Deleting data

Any discarded printed material containing personal data should be destroyed (by cross-cut shredding or to an equivalent state of unusability).

Data should not be kept when there is no longer a reason to do so. In particular, once data from paper forms has been transferred to computer records consideration will be given as to whether it is necessary (sometimes it is a requirement) to keep paper information, or whether it can be shredded.

g. Photographs

Photographs are personal data if a person can be recognised therein. Additionally, photographs posted on a website are by definition thus transferred worldwide. Permission from the Chief Executive / Assistant Chief Executive should be requested before publishing or posting photographs of living people.

If it is intended to take group shots at an event or function then participants must be made aware of this in advance, via clearly posted notices or announcements.

h. Audio/Video Recordings

If it is intended to record a meeting or an event then, at the least, an announcement to that effect must be made clearly specifying the future use which will be made of the recording. It is best practice to seek consent in advance, and where possible the agreement of all concerned, in order that anyone objecting to the use of recording devices is not prevented from participating in a meeting.

Recordings must be stored securely and wiped when no longer needed. In particular, care must be taken that a previous recording is not passed to a subsequent user of the recording device.

APPENDIX

Fire Officers' Association
London Road
Moreton-in-Marsh
Gloucestershire
GL56 0RH

Telephone: 01608 652023

Email: foa@fireofficers.org.uk
Website: www.fireofficers.org.uk

The Fire Officers' Association
Privacy Notice

May 2018

This Privacy Notice describes how the Fire Officers' Association, in its capacity as the data controller, collects, uses, shares, and keeps information about you in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the General Data Protection Regulation). This document forms part of the Fire Officers' Association Data Handling and Communication Policy (available from the FOA website or on request to Head Office).

Description of processing

The following is a broad description of the way this organisation processes personal information as well as a notice of your rights in relation to such information.

More information is available from the Fire Officers' Association's Data and Communications Policy or you may contact the organisation to ask about your personal circumstances.

Nature of work

The Fire Officers' Association operates as an independent trade union Trade Union within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992.

Reasons/purposes for processing information

We process personal information to enable us to provide a range of services to our members which may include administering membership records including the balloting of members and potential members; providing and organising activities for union members; promoting our services; supporting and managing our employees.

Type/classes of information processed

<u>Information Relating to Membership and Representation</u>

We process information relevant to the above reasons/purposes. This information includes:

- Personal details such as name, address and contact information
- Family details; where provided for payment of benefits
- Financial details necessary to enable collection of subscriptions
- Employment details, e.g. employer and role

In relation to requests for representation and support in connection with employment matters such as discipline or grievance it may be necessary to process sensitive information, such as: -

- Physical or mental health details
- Racial or ethnic origin
- Religious or other beliefs
- Trade union membership
- Sexual life
- Political opinions
- Lifestyle and social circumstances
- Information about offences and alleged offences
- Information about third parties as necessary in relation to the representation of members and their interests.

Under normal circumstances the above categories of sensitive information is not held directly by the Association but by persons or approved and legitimate third parties directly involved in the provision of representation, for example any appointed solicitors.

IP Addresses

Internet Protocol ("IP") addresses are automatically assigned to the computers by Internet service providers. An IP address may be identified and logged automatically in our server log files whenever you access our websites, along with the time of the visit and the pages that were visited. Your IP address may also indicate your approximate physical location. Collecting IP addresses is standard practice and is done automatically by many websites, applications and other technologies. IP addresses may be used for purposes such as calculating usage levels, diagnosing server problems or for verifying the uniqueness of online survey responses.

Information Sharing

Branch and Regional Officials

Information, limited to name, membership level, e-mail address, telephone number and employer(s) is securely issued to Branch and Regional representatives of the Association. Such information sharing is necessary for local identification of FOA members for communication and for conducting the business of a trade union.

Solicitors and Insurers

In order to provide effective advice and representation, all necessary information relevant to the matter for which assistance is required may be shared with the Association's principal solicitor, Slater and Gordon (UK) LLP, and any information imparted will be subject to their Privacy Policy (see https://www.slatergordon.co.uk/disclaimer/). Where a case is referred to the Association's legal insurance provider, Legal Insurance Management (LIM), information shared is subject to their Privacy Policy (see https://www.legalim.co.uk/privacy-policy).

The FOA Optional Insurance Scheme

Where applicable, information relevant for membership of the Association's optional Insurance Scheme and any claims made within the scope of that cover may include elements of the above sensitive information. Such information is processed, on the Association's behalf by Philip Williams and Company who provide and manage Scheme policies. Only information relevant to the effective operation of the Scheme or for processing claims is provided by the Association.

Where Philip Williams and Company deal directly with members, they will also have responsibilities relating to Data Controllers. Please visit the following link for more information - Link to Philip Williams Privacy Notice

Financial Information

In order to collect subscriptions or reimburse any due monies, it is necessary to hold details of members' bank accounts. Similar information is also required for officials and staff members to allow payment of wages and repayment of any expenses incurred.

A third party company, Eazy Collect Direct Debit and Card Processing Services, is engaged on behalf of the Association to collect subscriptions via direct debit. This company also provides a platform for gathering initial membership information as part of the online direct debit set-up process. Financial and personal data held and processed by Eazy Collect is subject to both the Association's and Eazy Collect's data policies (Link to Eazy Collect Privacy Policy).

In order to discharge statutory audit and accounting requirements, the Association's accountant and auditor (currently Samuels LLP) have access to data relating to members and staff. Their data control provisions are set out in the Samuels LLP Privacy Notice. (Link to Samuels LLP Privacy Notice).

Who the information is processed about

We process information relating to members only to the extent that is necessary to collect subscriptions and maintain access to FOA membership services.

Information relating to officials and staff is also held for the purposes of meeting legal requirements as an employer, for allocating tasks and for communicating information needed to undertake their duties.

Approval and Verification

Members must take positively action to consent to the Association holding their personal data. Without such consent, we are obliged to delete or stop using the information held. This would have the effect of resigning your membership as it would be impossible to collect subscriptions or verify entitlement to services and representation for matters arising from current or past membership.

In order to confirm the accuracy of membership records, a routine member details check is undertaken. From 1st June 2018, these checks will require members to confirm that they consent to their data being held and processed for membership and representation purposes. Members are strongly urged to respond when a details check is received.

Your rights as a FOA Member

Right to be informed

You have a right to be informed about the nature of the data held about you and how your personal information is used.

Right to correct information

You have a right to have personal information corrected if it is inaccurate and to have complete incomplete personal information.

Right to be 'forgotten'

You have a right to have your personal information erased.

Right to object to processing

You have a right to object to the processing of your personal information.

Right to withdraw consent

Anyone for whom the Association holds personal has a right to withdraw consent for its use at any time or to restrict and/or object to the use of that personal information.

Right to correct information
The right to have your personal information corrected if it is inaccurate and to have incomplete personal information completed

Right of data portability
You have the right to move, copy or transfer your personal information to another party.

Right to access data
You have the right to request access to your personal information and to obtain information about how we process it.

Automated decision making
Although the Fire Officers' Association does not use automated decision making systems, you have rights in relation to automated decision making which has a legal effect or otherwise significantly affects you.

Right to complain
You have the right to complain to the Information Commissioner's Office which enforces data protection laws: https://ico.org.uk/.

IMPORTANT NOTE RELATING TO YOUR RIGHTS

It should be noted that exercising a right that requires the erasure or restricted use of information relating to your membership may have the effect of ending membership with the consequences stated in the "Approval and Verification" section above.

Contact from the Association

You contact details will only be used to communicate for the purposes of issuing information relevant to your membership such as:

- Members' Updates and Circulars
- Consultation on matters relating to employment or FOA membership
- E-mail or letters relating to subscriptions and membership related services available or provided to members.

Marketing

The Fire Officers' Association will not provide any information relating to members to any third party for the purposes of sales or marketing.

Use of 'Cookies' and Other Systems that Collect Data Automatically

Subject to the exceptions listed below, the Fire Officers' Association does not use 'cookies' or mechanisms that automatically collect personal data.

- Capture of employment, contact and financial information via the online membership registration and direct debit set-up process,
- Website Registration where names and e-mail addresses are captured by the website user database for access authorisation purposes and password re-set when requested.

Data Retention

The Fire Officers' Association will only retain personal data for as long as that data is needed to fulfil the purposes for which that data was initially collected.

When personal information is no longer necessary for legal or regulatory needs or to administer membership services, we will take reasonable steps to securely destroy such information or permanently de-identify it.

We maintain strict requirements and security controls needed for identification, storage, protection, retrieval, retention and disposal of personal data.

Information about legal or financial transactions is retained for a period of 6 years in accordance with the general limitation period governing commercial contract law and our external contractors' terms of service.

For more information about our data retention practices, please contact the FOA Head Office.

Use of Data outside the United Kingdom

The Association does not operate outside the United Kingdom and will not, therefore, send or use personal information outside the United Kingdom.

Any information held in relation to members residing outwith the United Kingdom will be subject to the General Data Protection Regulation and FOA Data Policies.

Responsibilities of FOA Representatives, Officials and Staff

All officials and staff members are individually responsible for care in relation to these procedures, and for raising any queries, concerns or training needs which they might have.

On leaving any role within the Association, all records and data held by an official or staff member must be passed on to their successor or, in the absence of an identified successor, destroyed unless such material is unique in which case it should be sent to Head Office for safekeeping or disposal, as considered appropriate by the Chief or Assistant Chief Executive.

Queries and Complaints

If you have questions about this Privacy Notice, how your information is handled or wish to make a complaint or exercise your rights, call our Head Office on 01608 652023 or send an e-mail to foa@fireofficers.org.uk. You may also write to The Fire Officers' Association, London Road, Moreton-in-Marsh, Gloucestershire GL56 0RH.

Policy Review

The Association will routinely review its policies, procedures and documentation relating to the handing of information to take account of changes to processes or legislation; irrespective of which a review will be undertaken at least annually.