

# Data Protection Guide

## Data Protection Guide – Reps

As a union representative (Rep) you are implicitly agreeing to abide by the Union's responsibilities to data protection. You will have access to or will receive lists of members in your school and it is important use reasonable security measures to safeguard members' data at every stage until deletion or return to the Union, whichever is most appropriate.

This guide will highlight the core of your responsibilities. It is not an exhaustive list and will be updated as appropriate.

## Start of office

At the start of your role as a Rep carrying out the following should ensure a responsible approach to Data Protection.

- Read and understand and keep to hand this document on data protection making a note of where other supporting information can be found e.g. training course materials
- Read and understand the 'data protection statement' in Appendix A; as a Rep you have implicitly signed up to these
- Register and receive your official union access to download members' lists (when available)
- All devices where you may use, or store list of members must be password protected or ensure you have your own secure login if the device is a shared resource.
- **On receiving a list of members in your school you are not obligated to share this with your Head/Principal or anyone else, under any circumstances.**

## While an 'authorised' Officer

### Collecting, using and sharing members' data

#### Do

- Continue to adhere to the eight data protection principles as outlined in Appendix D.
- Encrypt or password protect all members' data files especially if stored in cloud storage facilities.
- Make note of your responsibility as per the data protection statement, Appendix A.
- Keep and use accurate and up-to-date members' data by regularly downloading and refreshing your core list of members from the national union; delete old lists including from the recycle bin.
- Regularly manage, by deleting or updating, members' data you may have uploaded to an on-line site e.g. on-line survey or bulk e-mailing applications
- Record and send to the national union all 'opt out' messages received from members following any marketing campaign or other on-line activity. E.g. uploaded e-mail addresses for surveys. See Appendix B
- Include the member's Membership Number when advising Records and Subscriptions (RSS) of updates/changes. This ensures the correct record can be identified.

# Data Protection Guide

## Don't

- Keep data for longer than is necessary – delete, especially if out of date
- Share data with 3rd parties unless they have signed a 3rd party agreement and can adhere to your strict terms and conditions when processing the data. Further advice must be sought from your local association/division or the Union for the guide 'Keeping members data safe while organising'
- Don't do anything that enables one member to see another member's data e.g. when e-mailing a group of members use the BCC field so e-mail addresses are hidden
- E-mail members' lists unless the attachment is password protected.
- Upload members' data to any on-line cloud storage unless it is encrypted; 'Folder lock' is currently ranked number one in the top ten encryption software.

## Devices: Laptops, PCs, tablets, iPads, smart phones, usb sticks

### Do

- Ensure all devices have password protected access and practice using strong passwords.
- Use good password practices e.g. never keep your ID and password details with your laptop
- Ensure all devices (mobile, tablets etc.) are secure using the security and privacy settings provided with the device.
- Shut down your laptop or workstation using the 'Shut Down' or 'Turn Off' option, never leave opened accessible devices unattended.
- Be aware of anyone viewing your screen as you enter passwords, view members' data or any other sensitive information

## 3rd party processing

It is your responsibility to use and share data responsibly. When working with 3rd parties or uploading data to on-line applications, use the minimum data needed to achieve the objective.

You are responsible for knowing where your data is, the versions shared and are in use.

### Do

- Ensure 3rd parties sign the non-disclosure – 3rd party agreements, which should include clear objectives and instructions on data processing. This is rare for a Rep, but should you need to do this ask for advice from your local secretary or the union for reference to the document 'Keeping data safe while organising'.
- Share the bare minimum data needed for your objective.
- Encrypt data before sending to an approved 3rd party for processing and ensure they encrypt any data returned.
- Encrypt all removable media (i.e. USB memory drives, CDs, portable drives) that may have members' data.

# Data Protection Guide

## Don't

- Store members' data in any cloud storage facilities e.g. dropbox unless encrypted
- Send sensitive information on removable media (i.e. USB memory drives, CDs, portable drives) without encrypting the data.
- Send sensitive information by email unless you encrypt, or password protect the file.
- Assume all 3rd parties will adhere to the agreement all the time; include seeds, i.e. an e-mail address which you have access to, so you can monitor any unauthorised usage of your members' data list.

## Paper Documents

### Do

- Securely lock away paper documents containing personal or sensitive personal data when not in use
- Secure any documents or notes containing personal information that would cause damage or distress if it were lost or stolen
- Shred all end of life paper records that may contain personal information using a criss-cross shredder before disposing in commercial bins

### Don't

- Leave documents containing personal information unattended anywhere
- Disclose documents containing personal information to people who do not need to see them
- Leave documents containing personal information on photocopiers, scanners, or printers
- Fax personal information unless you've pre-agreed the recipient will be at the recipient fax machine to confirm receipt. Check the fax number is correct.

## Leaving office

At the end of your role as a Rep there are some good practices you need to adhere to ensuring the Union can continue to fulfil its data protection obligations.

- Inform the local secretary and Union of your change of status
- All access to union facilities will cease
- All data you may have saved on any **personal** devices must be copied back to the association/division or Union and then deleted. This includes casework, relevant e-mails and paper files.
- Return all other members' data to the new Rep, local secretary or the association/division and delete all copies in your possession.
- You are no longer authorised to have, process or use any members' data.
- If you've outstanding casework and it is sensible for you to see these through to their conclusion, the steps above will apply at the end of each case. Casework data must be kept for 6 years following the end of a case.

# Data Protection Guide

## Appendix A

Data Protection statement

THIS DATA IS SUPPLIED STRICTLY IN ACCORDANCE WITH THE UNION'S DATA PROTECTION REGISTRATION AND THE INFORMATION IS FOR THE CONFIDENTIAL USE OF CURRENT AUTHORISED OFFICERS OF YOUR ASSOCIATION OR DIVISION ONLY.

THE DATA MUST NOT BE COPIED OR PASSED TO THIRD PARTIES. PLEASE ALSO BEAR IN MIND THAT MEMBERSHIP DATA IS SUBJECT TO CONSTANT CHANGE AND SHOULD YOU INTEND TO USE THE INFORMATION FOR A MAILING TO SOME OR ALL OF YOUR MEMBERS THEN ONLY VERY RECENTLY SUPPLIED DATA SHOULD BE USED.

## Appendix B

Reporting Opt-outs to the Union

Please report, as regularly as possible, any opt-outs from members received during on-line campaigns or bulk e-mailing.

Please note that opt-out is global and they would be excluded from all other communication excluding taking part in the democracy of the Union.

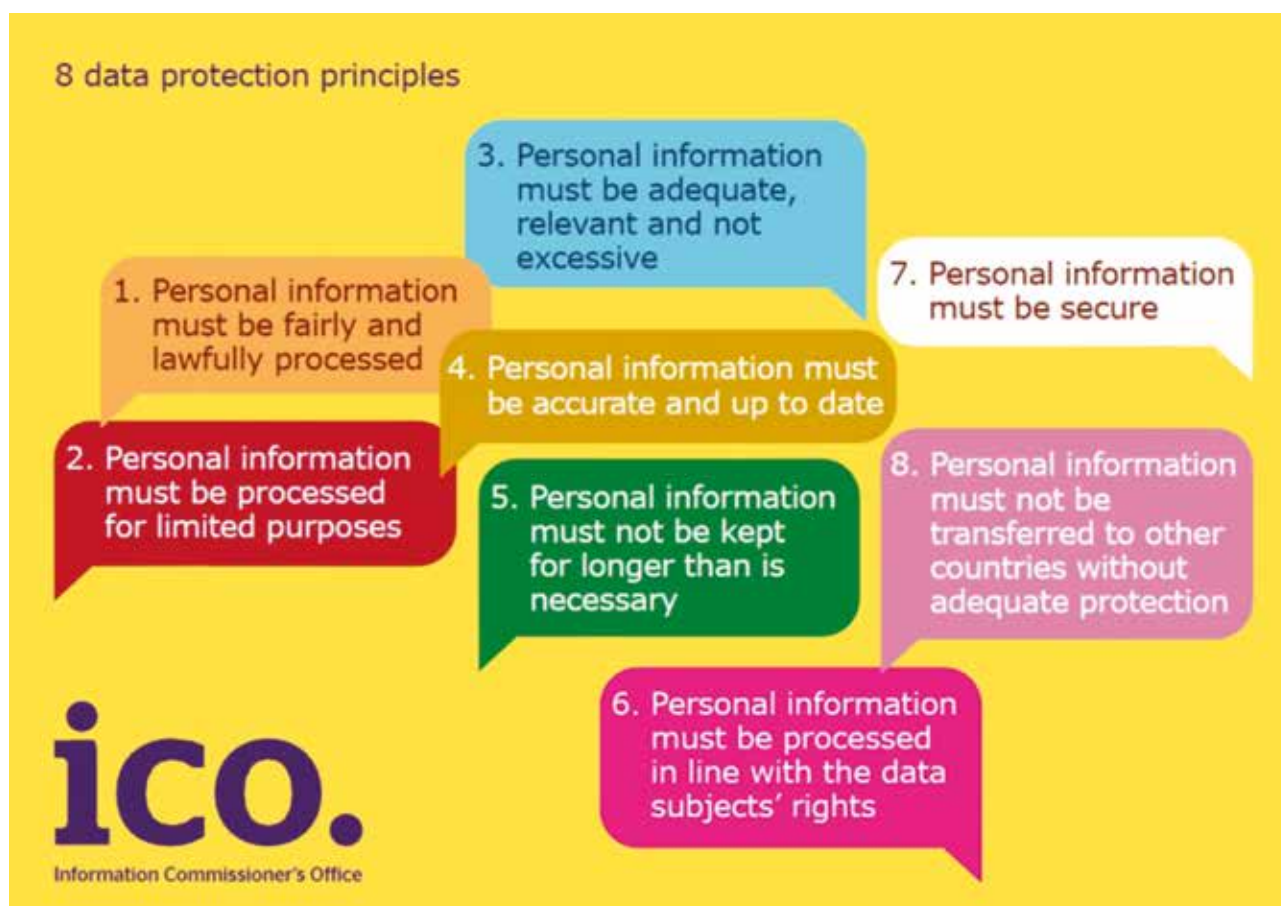
Members can elect to opt back in at any time. E-mail lists of 'opt-outs' to [RSS@nut.org.uk](mailto:RSS@nut.org.uk)

# Data Protection Guide

## Appendix C – Documents on Hearth – Not applicable

## Appendix D

### Data Protection Principles



# Learning notes

**Learning notes**

**Action points**