# Training checklist for small and medium sized organisations

## Data Protection Act

High-profile security breaches have increased public concern about the handling of personal information. As some 80% of security incidents involve staff there is a clear need for all workers to have a basic understanding of the Data Protection Act 1998 (DPA).

We recognise that some organisations have limited resources to devote to staff training. This note outlines some of the practical implications of the Act and is intended as a basic training framework for general office staff in small and medium sized organisations. Under each heading is a ***non-exhaustive guide*** to the points that should be covered in any training. Staff with duties such as marketing, computer security and database management may need specialist training to make them aware of particular data protection requirements in their work area.

## 1 Keeping personal information secure

Do your staff know:

- To keep passwords secure – change regularly, no sharing?
- To lock / log off computers when away from their desks?
- To dispose of confidential paper waste securely by shredding?
- To prevent virus attacks by taking care when opening emails and attachments or visiting new websites?
- About working on a 'clear desk' basis - by securely storing hard copy personal information when it is not being used?
- That visitors should be signed in and out of the premises, or accompanied in areas normally restricted to staff?

- About positioning computer screens away from windows to prevent accidental disclosures of personal information?

- To encrypt personal information that is being taken out of the office if it would cause damage or distress if lost or stolen?

- To keep back-ups of information?

## 2 Meeting the reasonable expectations of customers and employees

Do your staff know:

- To collect only the personal information they need for a particular business purpose?

- To explain new or changed business purposes to customers and employees, and to obtain consent or provide an opt-out where appropriate?

- To update records promptly – for example, changes of address, marketing preferences?

- To delete personal information the business no longer requires?

- That they commit an offence if they release customer / employee records without your consent?

- About any workplace monitoring that may be in operation?

## 3 Disclosing customer personal information over the telephone

Do your staff know:

- To be aware that there are people who will try and trick them to give out personal information?

- That to prevent these disclosures they should carry out identity checks before giving out personal information to someone making an incoming call?

- To perform similar checks when making outgoing calls?

- About limiting the amount of personal information given out over the telephone and to follow up with written confirmation if necessary?

## 4 Registration (notification) under the Data Protection Act

Do your staff know:

- Whether the company has registered with the ICO or is relying on an exemption?

- That you need to monitor changes in business use of personal information, and notify the ICO if appropriate?

## 5 Handling requests from individuals for their personal information (subject access requests)

Do your staff know:

- That people have a right to have a copy of the personal information you hold?

- How to recognise a subject access request?

- Who to pass it to if it is not their responsibility to answer?

- That the company has a maximum of 40 days to respond?

- That the maximum fee that can be charged is £10?

- That they may need to check the identity of the requester?

- What to do if other people's information is contained in the proposed response?

## Other considerations

Additional guidance is also available if you need further information on:

- Registration under the Data Protection Act: https://ico.org.uk/for-organisations/register/

- Getting it right - A brief guide to data protection for small businesses: https://ico.org.uk/media/for-organisations/documents/1559/getting_it_right_a_brief_guide_to_data_protection_for_smes.pdf

- Getting it right - Small business checklist: https://ico.org.uk/media/for-organisations/documents/1558/getting_it_right_-_how_to_comply_checklist.pdf

- Employment Practices Code – A Quick Guide: https://ico.org.uk/media/fororganisations/documents/1128/quick_guide_to_the_employment_practices_code.pdf

- CCTV Code of Practice: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

- Releasing information to prevent or detect crime: https://ico.org.uk/media/for-organisations/documents/1594/section-29.pdf

- Electronic mail marketing: https://ico.org.uk/for-organisations/marketing/

- Calling customers listed on the Telephone Preference Service: https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/telephone-marketing/

- Checklist for handling requests for personal information (subject access requests): https://ico.org.uk/media/for-organisations/documents/1599/subject-access-checklist.pdf

## Useful contacts

Federation of Small Businesses
Sir Frank Whittle Way
Blackpool Business Park
Blackpool
FY4 2FE
Phone: 0808 20 20 888
www.fsb.org.uk

Department for Business, Innovation and Skills
1 Victoria Street London SW1H 0ET
Phone: 020 7215 5000
https://www.gov.uk/government/organisations/department-for-business-innovation-skills

## More information

This checklist will be reviewed and considered from time to time.

It is a guide to our general recommended approach, although individual cases will always be decided on the basis of their particular circumstances.

If you need any more information about this or any other aspect of data protection, please Contact us: see our website www.ico.org.uk.