Trustees: A Brief Guide to Data Protection Risk

protecture
data protection office

Information Security

Who uses their own devices... and is this secure enough?

Working outside the office can be essential. It also forms part of modern working life. Yet the need for cost-effective solutions has seen an explosion in staff and volunteers using their own devices for work purposes. Your charity remains responsible for any personal information accessed via, and stored on, personal devices.

- Q Can any of your staff/volunteers use their own devices to access sensitive personal information – whether via emails or access to your systems? If so, what controls are in place?
- Q If a secure remote login is used, can staff/volunteers still save information to their personal unencrypted hard drives and/or memory sticks?

A City Council was fined £100,000 for their *"impractical and ambiguous"* Home Working Policy when it resulted in sensitive personal information being published to a public website in breach of the Data Protection Act.

Fundraising

Is transparency and fairness shining through?

Have your fundraising team presented to you.

- Q How they will seek fully informed, freely given, unambiguous (opt-in) consent for new donors; their assessment of the existing consents they hold and how they would seek updated consent if required?
- Q When they are not going to rely on consent for fundraising activities?
- Q A clear view of what they use donor data for, and how they will assess potential new uses of the data to ensure they always meet donor expectations?

The Leave EU campaign was fined £50,000 for buying data which did not have clear consent.
Pharmacy 2U was fined £130,000 for the unfair collection and use of customer data.

Suppliers

Could their actions cost you?

Suppliers can bring much needed expertise and savings. Your charity is responsible for ensuring (i) it selects suppliers who outline how they will handle your information and it then has contract clauses in place that ensure sufficient protection of the information.

- Q Do your contracts contain the minimum contract clauses mandated by the Data Protection Act?
- Q Do they also cover the full life cycle of the information, e.g. the secure return of data at the end of the contract?
- Q Have you audited your suppliers approach to handling your charity's personal information?

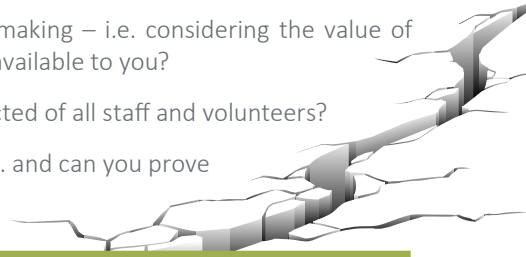
A hospital was fined £325,000 when a supplier – used to destroy redundant Hard Drives – passed the work to a sub-contractor without their knowledge... and they sold the Hard Drives, exposing sensitive medical data.

Governance

Are you doing all you can?

Your governance structure, and Data Protection policy and procedures, are essential to ensure staff know what you expect of them when they handle personal information.

- Q Are your policies based on informed decision making – i.e. considering the value of information; the risks faced, and the resources available to you?
- Q Do your policies provide clarity on what is expected of all staff and volunteers?
- Q Have you provided appropriate training to staff... and can you prove they understood what was expected of them?



Examples of outdated practice

Policy restating the law: *"we will be fair and lawful"*

Statements open to interpretation: *"staff should treat data securely at all time"*

Policy addressing only one area of the charity (e.g. HR data) and not key areas (e.g. Fundraising data).

No link between technical IT policies and other policy areas (e.g. procurement; fair processing).

How Protecture supports you…

Information Security

Use our expertise to develop robust, proportionate remote working/Bring Your Own Device policies.

Use our expertise to ensure your wider Data Protection policies address:

- Both electronic data and paper records
- Access to information – i.e. defined permissions based on the level of access required for the staff member to fulfil their role
- Backup of data and security of key paper records
- Handling requests for information – i.e. subject access requests; ad-hoc disclosures; Data Sharing Protocols and sharing with suppliers
- Procedures for handling security incidents
- Record retention and secure disposal

Fundraising

Have us review your fair collection/privacy statements:

- To ensure they are fit for purpose, and to prepare for the future legislative changes

Have us work with your fundraising teams to:

- Raise awareness of the future changes in consent, opt-in, and the Fundraising Preference Service
- Ensure clarity on the purposes for which donor data is collected and used, and the legal basis that underpins these uses
- Develop robust processes for when potential new uses of existing data are being considered

SUBSCRIBERS ALSO RECEIVE

- Free tickets to our seminars and events
- Regular updates
- Discounted hourly rates

Suppliers

Adopt our model *"due diligence"* questions in your procurement processes:

- To ensure you only select suppliers who provide sufficient assurances about their proposed handling of your information

Use our model contract clauses:

- To inform future negotiations and ensure you sign contracts that protect your interests

Have us audit your key suppliers – i.e. those that handle the largest volumes and/or sensitivities of personal information on your behalf:

- To provide assurance that your suppliers are meeting expectations, or otherwise working to a standard you are satisfied with

Governance

Have us deliver engaging, on-site training:

- We would tailor the training to the audience – e.g. whether Trustees, senior management, front line staff or volunteers

Use our self-assessment toolkit to assess your current compliance:

- We would provide feedback and recommendations, and would support you to deliver them

Use suite of template policies, procedures and checklists to assess any policy gaps:

- We regularly update these to ensure they meet any legislative changes

protecture
data protection office

acevo PREMIUM PARTNER

NADPO National Association of DP & FOI Officers

information and records management society

020 3691 5731 @protectureDPO help@protecture.org.uk www.protecture.org.uk