ico.
Information Commissioner's Office

Data Protection Tips/Pointers

Organisational measures

Training

- Evidence of training undertaken by all staff, monitoring of non-completion rates and processes in place to ensure this is followed up. Monitoring and enforcement of training attendance against corporate KPIs. *Consider blocking IT access where training hasn't been completed within satisfactory timescale?*

- Is refresher training available and, if so, on what basis? *Ideally, refresher training should be given on an annual basis.*

- Training itself to be reviewed regularly – to reflect lessons learnt and changes in procedures/policy and updates to reflect changes in practice – for eg – increased homeworking and use of mobile devices. *The best training often includes real life data breach examples.*

- Consider position of temporary/seconded/placement staff. Do not make assumptions that seconded/placement staff have received relevant DP training from their own employer. *Train promptly when they join your organisation.*

- Are effective, specialised training programmes offered for key roles e.g. Information Asset Owners including periodic refresher training?

Policies/Procedures

- Ensure policies are reviewed regularly and check to ensure that there is continuity across policies and departments.

- Ensure policies (or shorthand versions of policies) are read and understood by employees – consider a signed declaration by employees as part of an Induction checklist which is signed off by a manager.

- Ensure that policies are easily accessible to staff (website/hard copy/copy given on induction) and that key areas of policy and procedure are highlighted.

- Advise staff about any updates to policies or procedures (whole staff emails/thought of the day/staff bulletins on intranet etc.). Consider a rolling programme to raise staff awareness of DP issues rather than leaving it as just an Induction issue. *Hold an annual information security week?*

- Update/introduce policies to reflect changes in working patterns – mobile working/use of mobile devices etc.

- Consider a transportation of data policy/tracking procedure for when personal data is removed from the office? Do you know what is where, who has it and when it is expected to be returned?

General

- Making DP a whole staff issue – *clause in contract of employment making DP matters a disciplinary issue*.

- Consider use of an Induction checklist to ensure that all employees are clear as to what is expected of them and made aware of procedures relevant to their role. *Lack of awareness and supervision in relation to new/temporary staff are often contributory factors in a data protection breach.*

- Does the organisation have a robust data protection breach protocol in place? Do staff know about it, how to start the process and are confident about using it?

- Does data security feature in your organisation's disaster recovery plan?

- Consider whether there are effective controls of IT system access rights, including starters, movers and leavers protocols (permanent and contract staff) plus automated reconciliation with HR / payroll systems.

- Ensure administration staff are regularly reminded of need for care and consequences of breaches – greater the sensitivity of personal data the greater the need for care. Consider peer checking for very sensitive personal data where greatest risk of serious detriment. *A considerable number of breaches arise because inadequate checking processes are in place for basic administrative functions which deal with the most sensitive personal data.*

- Ensure new/inexperienced staff are supervised properly particularly if handling sensitive personal data.

- Retention of data – ensure procedures in place to review and archive/destroy personal data regularly.

- Consider a clear desk policy.

- Provide sufficient lockable storage to enable staff to protect hard copy personal data – lockers/cabinets.

- Consider whole building security.

- Consider spot checks – e.g. desks, work areas.

- Place posters above fax machines/coffee machine/printers to reinforce DP issues.

- Make DP a "live" issue with staff – DP champions within departments, Information Security Awareness days, regular discussion item on team meeting agendas. *Evidence of a process whereby breaches and near misses are analysed and lessons are learnt may be a mitigating factor when a report is made to the ICO*

- Consider Privacy Impact Assessments when planning any major project or system change where processing of personal data is concerned– eg relocation of staff/service or disposal of assets.

- Review procedures for confidential waste disposal, IT hardware disposal, storage and disposal of records where a third party is used to achieve this.

- Consider centralised control, monitoring and review of data sharing agreements.

- Ensure third party service providers are clear as to their DP responsibilities with regard to your organisation's personal data including the process to be followed in the event of a data protection breach.

Technical measures

- Is all personal data held backed up sufficiently and securely?

- Ensure effective network endpoint controls where possible and mobile device encryption, plus password control and enforcement.

- Ensure appropriate security controls for remote access and home working and check these on a regular basis.

- Consider disabling auto complete on Outlook.

- Excel spreadsheets – be aware of pivot tables and V and H Look up functions which may reveal hidden Meta data. *Particular issues have been identified when excel spreadsheets have been provided in response to FOIA requests or published on an organisation's website. Get your technical team to check the spreadsheet first for "hidden" data.*

- Check members of group emails on a regular basis to ensure they still need to be on the list. If attachments are regularly circulated (eg Excel worksheets which are constantly updated or added to) review the need to include and circulate all of the data particularly if some of it is historic.

- Redaction – ensure appropriate software is used – on Word you can reverse deletions even if subsequently save to pdf.

- Websites – Ensure have a procedure in place to regularly check for software updates and patches for third party software.

- Consider staging and testing before implementing any changes to websites and ensure changes and testing is recorded.

- Ensure completed "Contact us" forms, if used, do not remain on a website portal for too long a period and are archived regularly. Consider use of email contact as an alternative.

- Do you have an Information Asset Register and is the responsible person aware of the extent of their responsibilities and how to meet them?

Further information about the regulatory action taken by the Information Commissioner can be found as follows:

https://ico.org.uk/action-weve-taken/enforcement/

Please note that this list of tips is not exhaustive in any way and should not be seen as a checklist to be relied upon to ensure compliance by an organisation with its responsibilities under the DPA. It should only be viewed as a general indication of the types of issues that the ICO sees on a regular basis.