# Communication in a digital world

**Joanne Tibbott looks at how pension schemes manage and keep records of online communications and the legal requirements needed to protect themselves from any risks**

The Disclosure Regulations permit schemes to use electronic communications to give members information, whether by using electronic mail or by making information available on a website as appropriate, provided communications are designed to be accessible and capable of being stored and printed (taking into account the requirements of disabled persons).

Trust law requires trustees to use skill and care in the exercise of their duties and ensure good governance.  Legislation specific to running pension schemes also requires schemes to establish and operate internal controls which ensure they are administered and managed in accordance with required standards, meaning appropriate controls to identify, evaluate and manage risks of all sorts (including providing information to members and keeping good records) are imperative.

Any failure may ultimately result in The Pensions Regulator enforcing compliance under its statutory powers but, helpfully, guidance on key areas where internal controls and risk management strategies are necessary is available.

Both for reputational reasons and to ensure they are doing the best they can to achieve good member outcomes, trustees will want to be on the right side of appropriate record keeping and internal monitoring when it comes to resolving potential disputes about scheme information.

## Updating web-based information

Websites inevitably require updating and monitoring for accuracy and appropriateness. There could be routine changes to upload new scheme accounts or more bespoke changes reflecting alterations to benefit provision or updated legislation.

Trustees and their providers will need to take account of the circumstances of their own scheme and systems when establishing the appropriate level of control and risk management processes.

There is a myriad of possibilities given the number and types of schemes in existence but, as a minimum, schemes should undertake their own risk assessments and put action plans in place. Third party administrators should be able to help.

## Introduce controls

If there isn't already a system or process in place for managing digital material, consider introducing one. In any event, consider carefully what goes on the website in the first place. Who designs and monitors scheme information?  Who instructs changes to be made and how? Who checks the information on the website is accurate and how often?  Who is responsible for storage and archiving of digital material and how is that best achieved?

Consider recommending members print or save documentation or take a snapshot of information on the site at any particular point in time. The following wording might be suitable for some schemes: "After reading the literature within the links on this page, we recommend that you either save or print a copy and keep this safe for future reference."

The website should also warn information may be updated, so readers should check the date of material for accuracy.

## Digital archiving

As with all solutions, the range of options is wide. At one end, consideration could be given to providing only documents in pdf form archived online (with appropriate version control mechanisms) or in paper copy. Copies of screen pages could be saved every time there is an amendment (either by way of screen shot or as appropriate to the scheme).

At another level, IT solutions and software could be employed. Some websites capture old versions of websites for free, but these are not likely to capture every change and there is likely to be no contractual protection if something goes wrong (if it is hacked, for example, or data is lost). Evidence from Wayback machine has been admitted used in court in 2009*. Whatever is adopted, keeping audits and paper trails of developments is essential.

## Conclusion

Failure of operational and technical systems  resulting in breach of any delegated responsibilities  falls squarely at the trustees' door as far as members are concerned, meaning trustees need to have these issues in mind when considering internal control and associated risks. Data protection and cyber security are likely to also form part of these considerations, being inextricably linked with anything trustees do where information is shared and communicated electronically.

A new agenda item for your next trustee meeting perhaps?

*Plumbly v Beatthatquote.com Ltd [2009] EWHC 321 (QB)].

**Written by Joanne Tibbott, director in the pensions team, Gowling WLG**