Records Management and special category data

The Data Protection Act 2018 establishes “special category data” and records containing this type of information require the highest standards of management.

You can find out more about special category data on the Council’s Data Protection page but this includes information about the race, ethnicity, politics, health, sex life or sexual orientation of identifiable, living individuals. “Special category” is similar to the category of “sensitive personal data” under the previous Data Protection Act.

There are special conditions which have to be met for the processing of sensitive personal data (see the Council’s DP pages) and Data Protection defines “processing” of information very broadly, including its storage, transmission, retention and disposal.

These core information management functions should all be given extra care when dealing with special category data.

For example:

STORAGE:

special category data should never be held in a physical or electronic environment where it could be accessed by anyone other than those who have an appropriate business need to access it. Consider locked filing cabinets or secured drives; avoid open access paper systems or multi-access shared drives.

TRANSMISSION:

Special category data should never be sent to what appears to be a shared email inbox. Ensure that you have the correct email address and that the applicant agrees to its use. Care should be taken with unsecured internal mail envelopes: don’t use these for this type of data. Removable media should always be protected by passwords or appropriately encrypted.

RETENTION:

All information held across the Council should be held within an agreed retention schedule, defining how long it is kept and what is to happen to it and the end of that period. It is particularly important that the retention of special category data has due regard to this special status, that it is retained for no longer than it is required, and that the retention schedule is rigorously adhered to.

DISPOSAL:

Never dispose of special category information by anything less than a secure method. It must be confidentially destroyed by a reputable company with no possibility of its being found afterwards. This could mean onsite paper shredding or the secure and certificated disposal of computer hard drives or removable media.

While all these points could simply be described as good information management practice; do bear in mind the extra care which needs to be taken in relation to special category data.