National Association of Racing Staff

nars
National Association of Racing Staff

Document Retention Policy

Date; 4/02/2016 Signed; George McGrath, Chief Executive

Why?

It is the policy of NARS to ensure that documents and data are retained for the time required by the law or by funders.

Even where information is not covered by the Act, the Data Protection Act principles suggest that information should be adequate, relevant, not excessive, accurate, up to date and not kept for longer than is necessary.

Information/document type	Retention period
Trust deeds, governing documents	Indefinitely
Minutes of Executive Committee, Regional Committee meetings and AGM	Indefinitely
Health and safety assessments	Indefinitely
Insurance certificates	40 years
UL Project papers	10
Finance and salaries records	7 years
Team meetings 5 years	Funding paperwork 3 years after end of funding programme, or longer if the contract requires
Minutes and papers of meetings with external partners	1 year
Personnel records	7 years after employee leaves (reduce to information required for references only)
Contracts	6 years
Disciplinary records	6 months – 2 years depending on provisions of disciplinary policy
Employee time sheets	2 years

Job application forms for unsuccessful candidates, interview notes, disclosures	1 year
Accident book	3 years after last entry
Casework papers	7 years

Any other information kept by staff should be in line with the Data Protection Act and manual and computer records not listed above should be kept for no more than one year.

Information listed above which contains personal information should be kept securely and disposed of by shredding or some way which does not breach confidentiality.

DATA SECURITY PROCEDURES

All data and personal information (e.g. names and addresses, banks details etc.) should be kept confidentially and securely:

- Data in electronic form – in password protected areas and in encrypted form
- Data in hard copy form – locked away – office door to remain locked whilst unoccupied

Only those staff, volunteers and Executive Committee members that need access to this data for their duties should be given passwords or access to it.

Keep records of passwords in a secure place. The Office Manager is responsible for securing and updating passwords.

Key data for financial and wider security of The Chief Executive.