

# Important information about GDPR

## Handling Personal Data and Data Security

- Members should take appropriate technical and organisational steps to guard against unauthorised or unlawful processing. Manual records relating to members or others should be kept secure. Computer files should be password protected.
- The club will take particular care of sensitive data and security measures will reflect the importance of keeping sensitive data secure (definition of sensitive data is set out below).
- Club procedures will be regularly monitored and reviewed to ensure data is being kept secure.
- Where personal data needs to be deleted or destroyed adequate measures will be taken to ensure data is properly and securely disposed of. This will include destruction of files and back up files and physical destruction of manual files.  
**Particular care should be taken over the destruction of manual sensitive data (written records) including shredding.**
- All data will be stored in a secure location and precautions will be taken to avoid data being accidentally disclosed.
- Personal data stored on a laptop should be password protected.

## Compliance with the Legislation

Anyone who has responsibility for processing personal data must ensure that they comply with the data protection principles in the Legislation. These state that personal data must:

1. be obtained and used fairly and lawfully;
2. be obtained for specified lawful purposes and used only for those purposes;
3. be adequate, relevant and not excessive for those purposes;
4. be accurate and kept up to date;
5. not be kept for any longer than required for those purposes;
6. be used in a way which complies with the individual's rights (this includes rights to prevent the use of personal data which will cause them damage or distress, to prevent use of personal data for direct marketing, and to have inaccurate information deleted or corrected);
7. be protected by appropriate technical or organisational measures against unauthorised access, processing or accidental loss or destruction;
8. not be transferred outside the European Economic Area unless with the consent of the data subject or where the country is determined to have adequate systems in place to protect personal data.