Own Devices and Your Data: What Clubs Need to Know

Responsibilities

Personal devices used for club or organisational purposes may process personal data, bringing them within scope of the GDPR.

Data Security

Ensure personal devices are password-protected, encrypted, and kept up-to-date.
Avoid using unsecured apps or personal cloud services.

Communication

Organisations should use official communication channels whenever possible and delete chats once they are no longer required for club purposes.

Using WhatsApp groups

WhatsApp may be convenient, but it still involves processing personal data (such as name, messages, images, etc.). A club is responsible for ensuring its use complies with the GDPR.

Key Considerations

1. Only include individuals who have agreed to be part of the group
2. Make sure all members understand the purpose of the group
3. Never share sensitive information (e.g., medical details, vetting results, passports, etc.)
4. Switch off 'group invite links' to prevent unintended access
5. Review regularly and delete chats when no longer needed
6. Remove people who are no longer involved with the club

Policy and oversight

Sporting bodies should have clear 'bring your own device' and messaging policies, which explain:

1. When and how personal devices or messaging apps can be used
2. Security expectations
3. Procedures for loss or breaches

Regular training and guidance to coaches, volunteers, and staff should be provided.

If something goes wrong:

Report the lost or stolen device immediately to the club or person with responsibility for data protection.

Assess whether a personal data breach has occurred and act promptly.

An Coimisiún um Chosaint Sonraí
Data Protection Commission