****

**IT Policy**

Guidance Notes and Checklist

**Governance Code for Sport**

Disclaimer

Sport Ireland is making available a range of resources including guidance notes, policy documents and templates for selected areas aligned to the Governance Code for Sport which will support sport organisations, boards, management and staff in the development of relevant governance processes and procedures particular to their own organisation.

For the avoidance of doubt, the final decision on the nature, type, extent and format of approved governance policies, procedures and processes for each organisation is a matter for the board / highest governing structure of the organisation and the resources and material provided may assist the approval process.

This document is not, nor is it intended to be, a definitive statement of the law and it does not constitute legal advice.

This document is not a substitute for professional advice from an appropriately qualified source and it is recommended that sport organisations consult their governing document or obtain their own independent legal advice where necessary. Sport Ireland does not accept any responsibility or liability for any errors, inaccuracies or omissions in this document.

**Why an organisation needs an IT policy**

An Information Technology (IT) Policy identifies the rules and procedures for all individuals accessing and using an organisation's IT assets and resources. An effective IT policy is a model of the organisation’s culture, where good governance is underpinned by the rules and procedures around the volunteers and employees' approach to their information and work.

Principle 2 of the Code is about ‘Exercising Control over our Organisation’ specifically:

* Identifying and complying with all relevant legal and regulatory requirements.
* Making sure there are appropriate internal financial and management controls.
* Identifying major risks for our organisation and deciding ways of managing the risks.

Having a robust IT policy in place should answer each of these sub-principles and provide security around exercising control and managing risk. Furthermore, principle 1 (Leading our organisation), speaks of ‘Managing, supporting and holding to account staff, volunteers and all who act on behalf of the organisation’, while principle 5 (Behaving With Integrity) speaks of ‘Protecting and promoting our organisation's reputation’. Both of these principles will also be underpinned by an effective IT policy. All organisation types, whether A, B or C, need an IT policy in place.

An IT policy will cover such areas as General Data Protection Regulation guidance (GDPR),

data protection (derived from local laws), acceptable use of work email and internet, internet and email security and device security. It may also cover off IT procurement and training and off-site/working from home IT safety. The policy is a further opportunity for the organisation to communicate its values and culture and by showing it takes it responsibilities in this area seriously.

Whose responsibility is it to develop an IT policy?

It is the responsibility of the Board to ensure that all the principles of the Code are being upheld and delivered. The executive lead / Chief Executive Officer (CEO) is tasked with ensuring that the principles of the Code are being implemented in the organisation and thus will be responsible for ensuring an IT policy is written and being used internally. In an organisation with a HR manager, they will likely ensure that there is a social media policy, along with other HR policies, or it could be the responsibility of an IT Manager. In a volunteer led organisation there may be a volunteer with specific expertise in the area who will write the policy/guidelines.

What does IT include?

IT includes the following:

* Physical equipment (hardware) e.g., laptops and PCs / servers
* Virtualization e.g., cloud computing / shared systems
* Servers and storage
* Management of the overall system
* Security
* Networks
* Operating systems, and software (e.g., MS Word or a financial management package or a database) and applications (apps)
* User devices and peripherals e.g., mobile phones and tablets
* Other telecommunications
* Internet
* Websites and web portals

Basic IT management is about protecting data security. For example, all computers should be password protected and have up-to-date internet firewall and antivirus software. Staff/volunteers who use computer equipment on a regular basis should change their passwords and back up their files regularly. Part of core volunteer/staff training should include practices for digital protection, such as processes for identifying and dealing with malware and phishing emails.

All organisations are likely at a minimum to have in place an email server (their own or part of a larger server provider) with organisation specific email addresses and website domains registered. Broadly speaking, minimum IT requirements for an organisation will include: a server and robust/secure hosting platform for IT, PC or laptops for staff/volunteers, printers, LAN and broadband capacity to adequately serve the organisation’s needs (whether in an office space or ‘at home’). Thought needs to be given to all of this and how any risks involved in the use and management of these can be minimised.

What to include in an IT policy?

An IT policy is a way to ensure that everyone within the organisation knows their responsibilities when it comes to data protection and security. It should leave nobody in any doubt as to what aspects each section of the document covers, and which members of the organisation will be responsible for executing and enforcing it.

In Type C organisations this could mean designating overall accountability for IT and cyber security issues to a specific department or individual.

The document itself, meanwhile, should be clear about the scope of what each policy includes and how it should be deployed, with specific, action-oriented descriptions and step-by-step procedures placed alongside at-a-glance overviews for quick scanning. The IT policy should be updated regularly in line with evolving regulatory standards, and these revisions should be easily traceable.

**The following are elements that can be included in an IT policy:**

* A definition and purpose of policy: outline what the policy is about and that it applies to everyone
* The roles and responsibilities: who will take overall responsibility and how individual responsibility falls with everyone
* Acceptable use - detailing the circumstances under which the organisation’s IT resources can be permissibly used
* Confidential data - defining which information the organisation deems to be sensitive, and explaining how it should be handled
* Network access - explaining to staff and volunteers what procedures exist around device passwords, firewalls, networked hardware and wireless network usage, as well as covering what needs to be done to ensure security when connecting mobile devices
* Emails - outlining usage guidelines for the organisation’s email system to reduce the risk of any email-related security incidents
* Passwords - making sure that all members of staff and volunteers are adhering to consistent standards when it comes to selecting robust, confidential passwords that cannot be easily guessed
* Physical security - defining a policy for how physical devices are handled and transported, guarding against common risks
* Incident response - providing a step-by-step guide for everyone within the organisation to follow in the event that a breach does occur, with a focus on alerting the relevant parties, minimising the impact on network and data integrity, and recovering as quickly as possible
* New technology – needs assessment, procurement and implementation
* Adherence to national laws and privacy guidelines, as well as GDPR
* Protocols relating to the disposal of IT Assets

Implementing an IT policy: how and when to use it

New staff and volunteers should be made aware of all policies during the induction process, including the IT policy, and this should also be included in the employee handbook, and any introductory documentation given to volunteers. An IT policy, or updates to the IT policy, should be accompanied by training initiatives to make sure everyone within the organisation - from the Board, to the volunteers and administrative teams - know and understand these principles. The IT policy should be regularly reviewed – the Code states that policies must be reviewed every 3 years – organisations may choose to review their IT policy more regularly than that given that it is an area that is in constant development and is an area critical to security.

Further links and resources

[**Data Protection Commission**](https://www.dataprotection.ie/)

[**National Cyber Security Centre**](https://www.ncsc.gov.ie/)