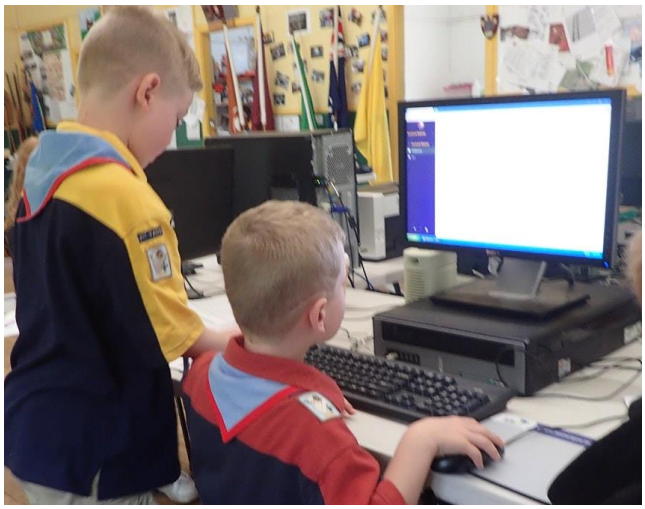
Technology Code of Use



P&R 5.2.3 Technology Code of Use

Adults and Youth in Scouting will use digital technologies including data, in a positive manner consistent with Scouting's Promise and Law, Code of Ethics, Code of Conduct, Child Protection Policy, Privacy Policy and legislated requirements including copyright, trade secret, patent or other intellectual property rights.

Technology Code of Use Standards:

Scouts Australia expects that:

- any device used for the storage of Scout information is password protected, and that password is changed regularly in accordance with Branch or National office requirements;
- passwords to access Scout information are of a reasonable security level (e.g. computer access requires a password that involves upper and lower case and at least numerals and/or characters in the authentication);
- Passwords to access Scouting information are not to be shared;
- all personal devices are stored securely and have a record of the device details (brand, model, serial number, etc.) that, in the event of theft or destruction, full details may be provided to the relevant law enforcement / insurance authorities;
- where peripheral devices are used for "back-up" purposes the same level of security and care will apply as for personal devices;
- all hard copy information held is stored in the most secure environment possible such as locked cupboard, office or premises; and

- a file name protocol that recognises the subject of the document, version number and date is used when saving a document. Marking as 'draft' and/or 'final' is optional.

Scouts Australia expects that Adults and Youth in Scouting will not:

- use their device to access, distribute or store unlawful material, or any other inappropriate material that could be considered counter to the Scouts Australia Code of Ethics / Conduct and the Scouts Australia Child Protection Policy, or bring harm to the Scouts Association in any way. Where there is any doubt, Adults and Youth in Scouting are to refer to their Branch Office for guidance.

In relation to its Technology Code of Use, Adults and Youth in Scouting recognise that Scouts Australia and its Branches:

- may take action to safeguard information and to block unwanted material that may bring the Association into disrepute, or, harm in any way;
- have a duty of care to protect Adults and Youth in Scouting and the organisation itself from malicious or unintended harm and may take action to fulfil this duty;
- maintain the right to take formal action against Adults and Youth in Scouting for negligence (in security), malicious or unintentional breaches of these principles (ranging from performance counselling to suspension or cancellation of membership or Scout employment); and refer matters to relevant law enforcement agencies.
- Recognises the right and responsibility of all Adults and Youth in Scouting to seek guidance as to their accountabilities to the Association and to each other. This guidance is available from your Branch Office.

Procedures:

The following procedures support Scouts Australia's Technology code of use policy:

- Within each Scout Formation, a responsible person is nominated to monitor that any shared Formation digital devices are secure with access only open to those requiring that access;
- Appropriate anti-virus software is installed and kept up to date to protect against the potential for Scouting information being hacked (or the like) and used for un-prescribed purposes;
- When interfacing with Scout owned software (e.g. Scout Central) Adults and Youth in Scouting logon details are to be kept safe and secure and are to be used only by the owner of that authentication.
- Not at any stage attempt to infiltrate (hack) or otherwise interfere with Scout Association software;
- Not violate the right of any person, business or Scouting's protected copyright, trade secret, patent or other intellectual property. Only purchased and authorised software is to be used for Scout management;
- Where possible, protect the transmission of another Adults or Youth in Scouting's details sent via email etc. This could be by password protecting files that contain personal sensitive information and using a different communication medium (e.g. Mobile SMS) when providing password details to the file sent by email;
- When seeking other personal information follow the protocols as set by their respective Branch. Some Branches have specific guidelines that must be followed when seeking data like mailing lists for reunions, Scout anniversaries and functions. This protocol ensures that the Branch will check the request is for bone fide Scouting purposes, or, part of the

allowable use of personal data contained within the Privacy Policy. This means that any Adult or Youth in Scouting cannot release information at their own discretion only. Above all else Adults and Youth in Scouting must verify and authenticate all requests for the provision of information. That is; Adults and Youth in Scouting will, to the best of their ability, confirm that requests for information is coming from an honourable, reputable and valid requestor;

- Ensure the establishment of any website or social media site is in accordance with Scouts Australia online technology and social media policies (and only on the approval of the Branch Office); and
- Where a Scout Association device has been provided for use comply with all additional policies and rules as defined by the Scout Association to which the device belongs (e.g. Branch Office).