

PRINCIPAL'S CHECKLIST* - MANAGEMENT OF SCHOOL ICT NETWORKS

*This checklist does not replace the requirement to follow all responsibilities outlined in the Education Policy and Procedures Register Policy.

GENERAL

- Follow, understand and communicate to staff, students and parents the major intent of the Using the Department's Corporate ICT Network Policy.
- Update and maintain the school's Network Usage and Access statement/guideline in line with the Using the Department's Corporate ICT Network Policy.
- Ensure students and parents are aware of policy intent and sign the school's network usage and access statement/guideline at least once prior to gaining network access (e.g. on enrolment, start of each school year).

Publication of Personal Information to School Websites

- Seek staff and parental consent before the publication of personal information to school websites, ensuring the consent form 'to use copyright material, image, recording or name' has been signed by the relevant staff member or parent/guardian of a student. (Refer to [LGS-PR-001: Consent to Use Copyright Material, Image, Recording or Name](#))
- Ensure restrictions are placed on access to a student's personal website developed through the school's network facilities or as part of the school's educational program. Restrictions can be placed on class, intranet (school) or internet (public) accessibility.
- Undertake a risk assessment, in order to define restriction levels to protect students personal information, considerations should include:
 - the type of information that should be published on the Internet;
 - use of web technologies (e.g. web cameras, chat rooms);
 - reasons for publication (e.g. outstanding achievements);
 - student situation (e.g. age; family situation);
 - identification of students (e.g. publishing group rather than individual photographs);
 - ability of others to digitally enhance published medium;
 - identify and removal of metadata that may be embedded within digital images;
 - ability of search engines to "crawl" the school's Internet pages and return results that identify students;
 - length of time that information is made available and should be removed after a minimum length of time;
 - amount of information about an individual that has been published over a period of time that may be used for profiling; and
 - information contained within documents e.g. newsletters, student work, etc, that are posted to a school website.

Connection of Private Devices to the Departmental Network

- Ensure departmental security measures are in place prior to allowing private devices network access and restrict access (e.g. printing, internet) for solely privately owned devices (e.g. non-EQ devices) connecting to the network.