

### **Special Education matters play such a prominent part of everyday school life. What can I do to protect the security of information and the privacy of my exceptional students?**

Be proactive. You will need to organize your department to address matters of security and confidentiality. Have a department-specific staff in-service early in the school year for Special Education Resource Teachers, Educational Assistants and others. This will assist your team, given the multitude of interactions that exist in the realm of special education: meetings, document exchanges, testing situations, health matters, etc.

**Principal's Best Practice:** Begin with the following checklist and then customize to suit your needs:

- Conduct yearly PIM in-service for Special Education Staff
- Conduct frequent internal audits of security protocols i.e. spot check one aspect of PIM per month
- As advocates are brought in, ensure a "consent to participate" form is completed
- OSR documentation files should always be kept current and accurate
- When personal information or records are exchanged, use appropriate "release of information" forms
- Protect super-sensitive documents such as those related to Kindergarten at-risk screening
- Securely destroy copies of documents that participants leave behind after meetings
- Encrypt/protect electronic files wherever possible
- SERT's must take care to work in a private area, limiting the exposure of computer screens, hard copy documents, etc. This would include having meetings in a secure, private location
- Provide quiet, unobtrusive testing areas. Discreetly invite students to testing sessions, thereby maintaining not only the security of information, but the dignity of the student as well