

# Digital Safety and Digital Citizenship

## A Guide for Students

The laptop has been given to you as a tool for learning. Use it for that. While doing so, here are some important rules for keeping yourself safe and being a good digital citizen. Most of them come from the Laptop User Charter you signed when you were given your laptop, which you can find at: [https://www.det.nsw.edu.au/policies/technology/computers/l4l/user\\_charter.doc](https://www.det.nsw.edu.au/policies/technology/computers/l4l/user_charter.doc)

Other sources include: <http://www.cybercrime.gov/rules/rules.htm>

### Digital Safety

Never let anyone else know your password. If you think someone else may have found your password, change it straight away.

Use passwords that no-one can guess easily.

Never let anyone else use your username and password. You may be held responsible for anything they do.

Always keep your laptop with you or in a very secure place.

Always log off at the end of each session to make sure that nobody else can use your e-learning account, just in case you do leave your laptop unattended or with someone else even for a short time.

Tell a teacher straight away if you suspect you have received a computer virus or if you receive spam or if you have received a message that is inappropriate, abusive, harassing or makes you feel uncomfortable. Do not reply to it.

If someone on the internet asks for personal information about you, asks to be telephoned, offers you gifts or wants to meet you, report this immediately to a teacher or parent. Do not give this information.

If you find any internet site that contains inappropriate material such as information or graphics that are sexually inappropriate, violent or racist, tell a teacher.

If you suspect that anyone has somehow got around the security of a laptop or the Department's network, report them to a teacher.

## **Privacy and Confidentiality**

Never publish or share the email address of a teacher or another student without that person's permission.

Don't reveal online anyone's personal information, including name, address, credit card details and telephone number. Only email or publish someone's photograph online with their permission.

Never forward emails or other messages without the sender's permission if they contain anything that was sent to you in confidence.

## **Cyber Bullying – No Way**

You have the right to expect others to treat you with respect online. Along with this you have the responsibility to treat others with respect. This means that you should never send or publish nasty comments about anyone or any abusive or offensive material. This includes:

- anything racist about anyone
- hurtful messages on social networking sites
- fake profiles or messages that are mean and hurtful
- false information about anyone or any organisation
- false or damaging information about a person or organisation
- messages or material that threaten, bully or harass anyone
- continually sending unwanted messages
- messages that make excessive or unwanted demands of anyone
- sexually inappropriate content in material or messages
- excluding anyone from an online group in order to hurt them

If someone does any of these things to you, you must report it to a teacher.

If you know someone is doing it to another student, you must report it to a teacher.

If you are found to be using the internet and online communication services to bully someone, you could face:

- the loss of access to email and/or internet services
- loss of laptop take home rights until you prove you are trustworthy
- other school fair discipline processes such as suspension

## Digital Citizenship

To be a good digital citizen you must not only look after your laptop, but also use it responsibly.

### Looking After Your Laptop

The laptop has been given to you as a tool for learning. Use it for that.

Charge the battery every night and bring it to school every day.

Keep it in its plastic case when you aren't using it.

If you stay at your present school or any other NSW public high school until the end of Year 12, you get to keep it. Until then, it belongs to the school even though you get to take it home every day.

Don't try to download any programs or games onto your laptop. It is packed with educational software. Other programs may badly affect the performance of your laptop.

Everything on your laptop can be looked at by school staff and other officers of the Department. The police can also ask to see anything on your laptop and anything you have backed up over the network.

Don't forget to back up your work regularly. Back it up to "My Locker" and somewhere else as well, for example, on a USB drive.

If you think it's been stolen, you must report it straight away to the police and they will give you an event number. You then report it to the school and fill in a Laptop Incident Form. You write the event number on the form. You and your parent/carer must sign the form.

Look after the laptop very carefully. You may not get a replacement if it gets damaged or it's lost. If it is damaged because you were careless or if you deliberately damaged it, insurance will not pay for it to be replaced or repaired. For example, if you trip and drop the laptop and its screen breaks, this is carelessness and insurance will not pay for the screen repair. In cases like this, you and your parents/carers may have to pay. This applies to your charger as well. If you refuse to pay, you will get a loan laptop which you won't be able to take home each day and you won't get to keep it when you complete Year 12.

If you do lose it or it gets damaged, one of your parents/carers must sign a witnessed statutory declaration, which is a legal document. If you don't know what this is, ask a teacher. You must also report the loss or damage to the school, give the school the statutory declaration and fill in a Laptop Incident Form which you and your parent/carer must sign.

If your laptop has to be replaced for some reason, it will be replaced by a laptop of a similar age, not the newest model.

## **Breaches of Security - Cybercrime**

### **Attempts to bypass filtering and other breaches**

All your use of the internet and online communication can be traced.

Your access to the internet is filtered by the DET, both at school and at home. This is for your safety.

You will be found out if you:

- try to get around the filtering of the internet by, for example, using a proxy server
- access inappropriate sites
- create, participate in, or share material that attempts to hack into and/or bypass the laptop hardware and software security
- break the Laptop User Charter in other ways

Your principal will receive the details and you will be interviewed and warned never to do it again.

If you are found to have done this again, your Principal will be told, you will be interviewed and your laptop taken from you. You will be issued with a loan laptop while yours is sent away for investigation and possibly to have it returned to its original state. If the investigation finds that you have broken the user charter, you will be disciplined. This may include, but is not limited to:

- the loss of access to email and/or internet services
- loss of laptop take home rights until you prove you are trustworthy
- other school fair discipline processes such as suspension

### **Tampering (interfering) – a more serious breach**

If it is found that you have tampered with your laptop's hardware or software, for example to give yourself administrator rights, this will be detected and your laptop will be shut down. Your Principal will be informed, you will be interviewed and your laptop will be taken from you. You will be issued with a loan laptop while yours is sent for investigation and possibly for repair and to have it returned to its original state. If the investigation finds that you have broken the user charter, you will be disciplined. This may include, but is not limited to:

- the loss of access to email and/or internet services
- loss of laptop take home rights until you prove you are trustworthy
- other school fair discipline processes such as suspension

### **Viruses, spam and other things**

Never send emails or other messages containing:

- a computer virus or attachment that can damage computers.
- chain letters and prank emails.
- spam, e.g. unwanted advertising material.

Don't use your laptop for money-making activities, online gambling or any illegal purpose.

## **Intellectual Property and Copyright**

Don't make copies of material you find on the internet and pretend it's your work. This is known as "plagiarising". Always acknowledge the author or source of any information you use in a bibliography. Your teacher and the librarian can explain how to do this.

Always gain permission before electronically publishing anyone's work or drawings. Always acknowledge the creator or author of any material you publish.

Make sure that any copyrighted material you publish on the internet or local school network has the approval of the principal or a teacher. A teacher and your librarian will be able to tell you about copyright.

Don't steal copyrighted computer programs ("software"), movies, TV shows and games by copying them from the Internet. This is the same as stealing them from a store. People work hard to develop new programs and deserve to be paid for them. If software designers and others don't get paid for their work, they can't continue creating things such as new software, new games or educational tools that help with schoolwork.

## **Breaking the Laptop User Charter**

You will be held responsible for your actions while using the laptop.

You will also be held responsible for anyone who breaks the Laptop User Charter while logged on to your e-learning account.

Misuse of internet and online communication services and breaches of the Laptop User Charter may result in disciplinary action which includes, but is not limited to:

- the loss of access to email and/or internet services
- loss of laptop take home rights until you prove you are trustworthy
- other school fair discipline processes such as suspension