Shire of Dardanup
Library Services

eSmart Facts Sheet

What is an eSmart Library?

The eSmart Libraries program provides a framework for developing digital skills and cybersafety for library staff, users and the community.

Why do we need to be eSmart?

This is a great opportunity for library staff to increase their own digital literacy and awareness of cybersafety and to assist people of all ages to avoid

- **scams,**
- **computer fraud; and**
- **invasions of privacy/bullying.**

Library staff are guides helping library users to navigate the digital world. As the digital world and digital devices are constantly changing we need to update our skills and be aware of current scams and cybersafety issues

While Shire of Dardanup Library Services will provide information via training, internal emails and blogs, staff should keep themselves informed through magazine articles (eg: Choice magazine), email alerts, social media or RSS feeds.

How did it start?

eSmart Libraries was initiated by a partnership between the Telstra Foundation and the Alannah and Madeline Foundation (a national charity protecting children from violence and bullying).

Library services who would like to gain eSmart accreditation follow a particular process developed by the eSmart national office. Although libraries may already be carrying out some aspects of eSmart, the tools and frameworks provided help busy libraries to follow this process in a methodical way.

An associated eSmart schools program is running in about 1,500 schools. eSmart is working with a similar number of libraries across Australia.

‘eSmart Libraries will help build skills and behaviours for the smart, safe and responsible use of technology, contribute to digital inclusion and foster a greater sense of wellbeing for the library community.’

Components of eSmart

1. **Vision, strategy and leadership**
2. **Library agreements and procedures**
3. **Staff knowledge and capabilities**
4. **Guidance and Learning for Users**
5. **Community connections**

Key Areas for Staff:

Cybersafety

Staff are expected to understand the key elements of cybersafety relating to:

- **scams**
- **privacy settings on digital devices and social media**
- **cyberbullying**
- **importance of anti-virus and software updates**
- **use of passwords**

Scams

Easy ways to identify scam emails include:

- **incorrect email for that institution/company, eg: apple@bzxy.net**
- **bad spelling or grammar**
- **email that claims that an account will be suspended if no action is taken**

It's advised that staff sign up for the Stay Smart scam email alert service, a Federal Government initiative at http://www.staysmartonline.gov.au/ This helps you to keep up to date on scams that borrowers might be receiving on email or by phone.

There are several scams that are recycled each year by scammers.

Nigerian scam:

Scams such as the so-called ‘Nigerian Scam’ distribute emails purporting to be from someone who has a large sum of money that they ‘temporarily need help with’ ie by using someone’s bank account.

This type of plea is used to gain a person’s bank account or credit card details. Because of the sheer number of these emails sent out there are always a few people who are vulnerable enough to believe that the scam email is authentic. Most people who work in libraries will see this scam in its various forms.

Dating and Romance scams:

Preying on the vulnerable, attempting to get people to divulge personal details and send money. This is a still a common scam through which scammers earn millions of dollars a year from Australians.

Scammers are also developing new ways to defraud people eg: Ransomware: Individual or company files are encrypted so that users are locked out of their files. Scammers ask for ransom money to allow access to files. The delivery of these scams ranges from malicious email attachments (often zip files), ads on websites or convincing people they need to download apps from unknown sources. Individuals are sometimes asked to pay the ‘ransom’ with Bitcoin, an alternative web currency.

Staff Tip: ***Recommend to library users to ignore suspicious emails, especially when they contain attachments. Never open the file or download the attached files.***

Phishing:

Requests for personal or company information by scammers posing as legitimate institutions or businesses. These scams may be carried out via internet or SMS text messaging. Websites may use copied logos and links that look similar to the company’s own website address or URL.

Staff Tip: ***Financial institutions will never ask you via email to provide your personal information and account details.***

Microsoft or Telstra scam:

People pretending to be representatives of Telstra or Microsoft call random people saying, ‘Your internet account has been hacked’ OR ‘There is a problem with you internet connection’ OR ‘Your computer needs fixing’. If they don’t take the action recommended (i.e. following steps to download software or something similar) their online banking will be compromised. These scammers are convincing and provide false ringback numbers. Victims lose money from their online banking or bank accounts if they give out their information.

See more at:
http://www.scamwatch.gov.au/content/index.phtml/tag/requestsforyouraccountinformation For a
http://www.staysmartonline.gov.au/your_identity/avoiding_scams_and_hoaxes

Recognising secure websites

One way of recognising a secure connection is useful, eg: especially for online shopping. In the browser website address bar you should see https: and possibly a lock icon instead of the usual http: The 's' indicates that the website is encrypting information being sent to and from the website so that computer hackers will not be able to easily access the information.

Clicking on the padlock gives more information about the authenticity of the website.

More ways of checking if websites are dodgy:
https://www.thinksecurityguide.com/your-family/recognizing-and-avoiding-fake-websites.aspx

Privacy

Social Media

Social media can be fun and useful for information-sharing but can also make people vulnerable to invasions of privacy or at worst can put them into life-threatening situations.

Staff tip: ***Check the privacy settings for all your social media platforms. If you go to account settings on social media websites such as Twitter you can choose various levels of privacy.***

Resources for learning about social media concerns and privacy settings:
http://www.staysmartonline.gov.au/socialising_online
https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

Cybersafety resources

Some key points to ensure cybersafety:

- **secure passwords**
- **anti-virus program installed on computer/devices and**
- **up to date version of computer software.**

Software updates, antivirus and other e-security

It is essential to install and update anti-virus and other e-security software to restrict unauthorised access to data on computers and mobile devices.

- **Ensure that security features including a firewall are turned on, set to automatic scan and updated regularly to protect against the latest risks. If cost is a factor, basic anti-virus software is available, although the 'paid for' services may have more features.**

A good starting point for resources relating to cybersafety can be found at the Monash Public Library website: http://monlib.vic.gov.au/eLibrary/Our-Training-Notes/Cybersafety

Passwords

There are many common passwords that people use, such as 1234. Hackers are aware of these common passwords.

For more secure accounts consider two factor authentication: http://lifehacker.com/5938565/heres-everywhere-you-should-enable-two-factor-authentication-right-now

For more information about passwords visit: https://www.thinksecurityguide.com/Your-Digital-Assets/Password-Security.aspx

Cybersafety for Children

Occasionally a customer may request for 'safe searching' to be enabled on the public PC that they or their child are using.

To enable safe searching in Google, follow these steps:

1. **Click on the cog on the right hand side of the Google screen.**
2. **Visit the Search Settings page.**
3. **In the "SafeSearch filters" section, select or unselect Filter explicit results.**
4. **Click Save at the bottom of the page.**

Alternatively, you can direct customers to open this site: http://www.safesearchkids.com which is a site set up by Google which helps remove potentially explicit material from appearing in Google search results. It also gives a wonderful explanation of why 'safe search' is important and would be a great resource to recommend to parents who express concern about this.

The StaySmartOnline site provides links to resources to assist young people learn about cybersafety and cyberbullying. You can also find anti-bullying resources for teachers, students and parents at: http://bull yingnoway.gov.au/

For more information visit:
http://www.cybersmart.gov.au/tagged.aspx
https://www.esafety.gov.au/

Staff Digital literacy skills

Social media, internet, digital devices

Being eSmart is a very important part of our role working with the community in public libraries. We will only begin to be eSmart if we have a reasonable level of digital literacy. This means being comfortable engaging with a wide variety of technology and ensuring that we regularly assess our own knowledge and competencies.

eSmart topics will be discussed in team meetings and supported through library training courses for staff and users. You are also responsible for ensuring that your knowledge is up to date. The following resources provide a wealth of information to support general staff literacy.

As borrowers look to library staff for assistance with using digital devices, we need to be familiar with the basics of mobile devices and the use of e-readers and tablets - especially for utilising library e-book collections. Make sure as a staff member you are familiar with the iPads we offer to library members to use, how to access key features such as camera, ebooks, and internet browsing and what our terms and conditions of use at the end of this document.

ForwardIT: http://www.forwardit.sa.gov.au/home

> *This website helps you to learn how to use the internet safely and securely. It features videos and information presented in an easy-to-read format and you can learn at your own pace. It covers 'online' basics really well and is a great starting point if you don't feel tech savvy.*

WebJunction: http://www.webjunction.org

> *This is a website that is library specific and contains numerous resources explaining digital literacy. If you click on: Explore topics > Library Service > Digital Literacy > Webinars, you will find a great selection of resources that not only teach basic digital literacy skills but they also teach library staff how to teach these skills to customers.*

GCFLearnFree: http://www.gcflearnfree.org

> *This website provides a wide variety of free online tutorials under the banner of Technology. It includes tutorials on: devices, computers (Mac & Windows), social media, Google Cloud, graphics/photos, online safety and general digital skills.*

Shire of Dardanup
Library Services

eSmart Facts Sheet

Library technology use agreement:

The Shire of Dardanup Library Services is committed to providing library users with the skills they need for smart, safe and responsible use of technology and we provide a range of opportunities for accessing information including on-line through free access to the internet via PCs, Wi-Fi and also iPads.

The procedure below provides a guideline for acceptable use of public internet access computers and Wi-Fi while promoting the eSmart philosophy and apply to any one accessing public computers, internet and electronic resources provided by the Shire of Dardanup Library Services. Full details of this policy can be made available upon request:

Access

- Public access to computers, iPads and Wi-Fi is free of charge.
- Printing is charged for in accordance with the Library's Fees and Charges.
- To ensure equitable access, time limits apply as the public access computers are often heavily used.
- While every effort will be made to provide assistance to users of the computers, it is assumed that customers booking public access computers will have basic computing skills. Assistance and information regarding training options are available from library staff.

Property

- Customers wishing to borrow a Library iPad must be at least 18 years old and provide a valid library card and driver's licence which will be kept at the service desk for the term of use.
- Library iPads are not permitted to be taken from the Library for any reason.
- If a user wishes to listen to media on a public PC it is their responsibility to ensure they have the appropriate hardware to listen with (eg. headphones or earphones).
- The Library Service assumes no responsibility for any damage, direct or indirect, arising from use of the internet including viruses, adware or spyware.
- Customers are not permitted to damage, modify, add or delete software or tamper with computer, iPad or printer settings in any way.
- Work cannot be saved on library computers. Customers wishing to keep their work should save it to their own external device (eg. thumbdrive or hard drive).

Children & Parents

- The Library Service promotes and supports young people's access to information, including electronic information through its internet facilities. Library staff are available to assist children in the use of the internet and to recommend websites on particular subjects.

- Parents or guardians are responsible for their children's access to and use of the public computers and Library iPads including access to sites, their subject matter and content.

- Children under 12 years old are not permitted to use the public computers unless directly supervised by a parent or legal guardian.

Right to Privacy

- It is the user's responsibility to ensure that any sensitive documents or information of a personal nature are removed from the computer when their session is finished. This includes signing out of any personal and secure logins (eg. Facebook, Gmail etc). The Library Service cannot guarantee security and confidentiality of any transaction, particularly e-commerce and internet banking transactions.

- The Library Service respects the rights of individuals to privacy; however, access to internet facilities is provided in a public place and through publicly available facilities; therefore, no guarantee of privacy can be made.

- Customers should be sensitive to the values and beliefs of others when displaying potentially controversial information or images on computer screens located in the library.

Responsibility and restrictions

- Customers are responsible for abiding by all copyright, censorship and other relevant laws and legislation when accessing, posting, forwarding, saving and/or printing materials.

- Customers are not permitted to advertise, transmit or request objectionable or restricted materials.

- Customers using public access computers and Wi-Fi must adhere to the Library Internet Policy, Conditions of Use, the Library General Use Agreement and this procedure. In the event of any breach of the Conditions of Use, the Library Service reserves the right to immediately terminate the use of the service and to maintain that restriction for as long as the Library Service chooses. Where such use includes suspected illegal activity the matter may be referred to the Western Australian Police.