

eSmart Libraries- Staff Training Plan

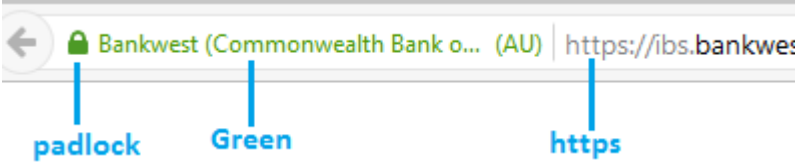


As discussed, you will receive one email every week for the next four weeks which will assist in developing your knowledge surrounding smart, safe and responsible use of technology.

Please read, review and complete the activity outlined in the brief email and bring your points along to the staff meeting for discussion.

Week 1	<p><i>eSmart Libraries – Staff Induction – An Overview</i></p> <p>Please put aside 15 minutes some time during the week to complete the below.</p> <ol style="list-style-type: none"> 1. Look at ESmart Libraries website 2. Read the benefits of eSmart libraries. 3. Why as an organisation should we continue to undertake the journey towards becoming an esmart library? 4. What do you hope to learn through this training?
Week 1	<p><i>eSmart Libraries - Staff Education – The Basics</i></p> <ol style="list-style-type: none"> 1. Take a look at the Library Website 2. Where can you find links to useful external sites? 3. What is the main emphasis of one of these external sites?
Week 2	<p><i>eSmart Libraries - Staff Training</i></p> <ol style="list-style-type: none"> 1. Access this link: eSmart Libraries Staff Training There are 8 modules, approximately 15 mins each which comprise an intro, a short video or link to an external site, and a 3-question quiz. 2. Complete the Checklist on the 2nd page and bring to the staff meeting on 13th November 2017
Weeks 3	<p><i>eSmart Libraries - Assisting Internet Users</i></p> <p>External cyber and digital literacy resources</p> <p>After completing the online learning, you will feel more confident in guiding patrons and library visitors to external websites providing best practice and up-to-date information on cyber safety for various user groups. Sections include Young People, Online Reporting Channels, Learning Tools.</p> <ol style="list-style-type: none"> 1. Go to the public facing area of the eSmart website by accessing www.esmart.org.au Look for: eSmart Libraries/ Cyber and Digital Literacy Resources. See dropdown menu below. Or click here <ul style="list-style-type: none"> • Which site(s) would you recommend to a patron who has limited experience of the internet, either new users or older users?

Weeks 3	<p><i>Copyright</i></p> <ol style="list-style-type: none"> 1. Please head to www.copyright.org.au. 2. Select "Browse from A-Z" from the footer. 3. Scroll down to L to find copyright information on libraries. 4. Select one information sheet that interests you and jot down the name of it to bring to the staff meeting. <p>Does the photocopier at our workplace display the Warning notice which we must provide to our customers?</p> <p>There are also some interesting items that relate to digital copyright and downloading.</p>
Week 3	<p><i>Social media and reputation management</i></p> <p>Looking at what can go wrong and the steps people can take to decrease risks and manage their online world in a more private way.</p> <p>Take a look at www.thinkuknow.org.au. The website has two sections; one for parents/carers and one for young people 11-17. We will mainly look at the teen section this week.</p> <ol style="list-style-type: none"> 1. Name one thing that can go wrong online. E.g. Online Grooming 2. Identify one step that can be taken to avoid this E.g. Only accept friend requests from people you know and trust. <p>Also an excellent resource for teens is www.cybersmart.gov.au/tagged</p> <p>Don't forget to bring your answers to the staff meeting for discussion.</p>
Week 3	<p><i>Social networking</i></p> <p>Where can you find Facebook tips and tricks on how to best secure your account and ensure safe socialising?</p> <p>Have a go at trying to locate this information and bring suggestions to the staff meeting.</p>
Week 4	<p><i>Reliable Information</i></p> <p>How can you identify that information available online is reliable?</p> <p>A few things to look out for:</p> <ul style="list-style-type: none"> • Last modified date. • Who published the site? • Who is the author and what credentials do they have? • Beware of bias. • Are sources visible? • What does the URL indicate? <p>Much can be gathered from the URL. http://www.domainregistration.com.au/ Did you know that .wa.edu.au is for WA education institutions only?</p>

Week 4	<p><i>Secure Sites</i></p> <p>How do I identify if a site is secure? Look for:</p> <ul style="list-style-type: none"> • a locked padlock or key symbol at the top or bottom of your browser window (outside of the web page itself) • a web address that starts with 'https' instead of just 'http' in your browser address bar. • a browser address bar that turns green • a security policy detailing measures taken to protect your personal details, including: <ul style="list-style-type: none"> ○ the level of encryption used in the SSL process – 40-bit is the minimum ○ whether the business sees and stores credit card details, or they are transferred directly to a bank ○ how long the business stores credit card details and how it protects them against external hackers and its own employees <p>http://www.commerce.wa.gov.au/consumer-protection/scams-and-security</p> <p>Example of secure site.</p> 
Week 4	<p><i>Scams</i></p> <ol style="list-style-type: none"> 1. Find a Scam example that you think is interesting on www.scamwatch.gov.au or www.afp.gov.au 2. Email the title of the Scam to me. 3. We will discuss a couple of them at next week's staff meeting.