



cyber(smart:)

## Hector's World™—Lesson Plans Information for teachers

### INTRODUCTION TO HECTOR'S WORLD™

---

Hector's World™ Limited has developed a range of free resources to help educate and protect children online. These resources feature New Zealand's Cybersafety Ambassador, a very cute bottlenose dolphin named Hector Protector®. Hector and his friends Ranjeet™, Sprat™, Ming™, Tama™, Kui™ and Constable Solosolave™ live in 'Silicon Deep', an underwater world which acts as a metaphor for the online world which is so familiar to many young people today.

The learning objectives of Hector's World™ education include components of information literacy, digital literacy, media literacy, as well as cybersafety and security. All of these components are part of the broader focus of digital citizenship—offering a good foundation of knowledge and skills to young children when they first use ICT can help them mature into confident and responsible digital citizens.

Hector's World™ lesson plans are designed to be used in conjunction with the animated episodes posted on [www.cybersmart.gov.au](http://www.cybersmart.gov.au).

*Episode 1: Details, Details...* is the Hector's World™ pilot episode, which offers a good introduction to our characters and the setting for our stories. There are important cybersafety points in this pilot episode and we've offered lesson plans to further the learning outcomes. Episodes 2-5 continue the development of important cybersafety themes, particularly around personal information online. We recommend that you use episodes 2-5 together and you can start with the pilot episode if you wish.

### AIM OF THESE LESSONS

---

By completing this module, students will gain an understanding of the importance of only divulging their personal information to people they can trust. Students in these year levels should have an appreciation of who such people are, which is usually dependent upon how well they are known to or integrated into their family, or their position in the community (for example, police officers or teachers). As such, these lessons emphasise the importance of listening to and acting upon one's uneasy feelings when assessing whether a person or situation is safe, and always seeking guidance from a trusted adult.

The latter lessons in this module also reinforce the importance of children turning to a trusted adult for support when faced with an online situation which they find upsetting or unsafe. Having identified such people in the module's earlier lessons, this equips students with a practical skill designed to enhance their personal safety in both the offline and online world.

---

## EPISODE SUMMARIES

---

**Episode 2: Welcome to the Carnival**, sees Hector and his friends arrive at a carnival. There, they encounter situations in which they have to decide whether certain characters they meet are able to be trusted with something very unique and special: their personal information. The friends rely on one another to help make these decisions, but only time will tell if they are the correct ones.

**Episode 3: It's a Serious Game**. Hector and his friends find that in order to play games at the carnival, they must divulge their personal details to a character whom they suspect is not trustworthy, the Squid. The friends differ in their decision about whether to do this, which may have repercussions for their future enjoyment of the carnival.

**Episode 4: The Info Gang**, begins with one of the friends discovering that the personal information that has been gathered during the carnival is being misused by the Squid and his henchmen 'The Info Gang'. Hector and his friends are able to bring the gang to justice with the help of Constable Solosolave, but Hector still has misgivings about his decision to divulge personal details to the gang before he knew they were up to no good.

**Episode 5: Heroes**, sees our young friends rewarded for their part in capturing the Info Gang. Hector is able to discuss with Kui his regret about divulging personal information to the gang. Kui gives him some valuable information about how to keep safer in the future.

## DELIVERING THE LESSONS

---

Each lesson should take around 45 minutes. Some of the lessons involve worksheets that reinforce the teaching points within the lesson. Some students will complete these more quickly than others, but it is not necessary for each worksheet to be completed before moving on with the next lesson.

We suggest that you view ALL of the episodes first, and review the key cybersafety points (below) in case they come up in class discussion.

At the beginning of lessons 3, 4 and 5, you can briefly review the storyline and teaching points from the previous episode. There is a set of character flashcards on the Cybersmart website which are referred to at various times during the lessons. These can be displayed in the classroom for the duration of the module.

## USING THE EPISODES

---

Flash Player needs to be installed to enable viewing the episodes. The episodes may be viewed on Windows or Mac-based computers with a broadband connection to the internet.

These lessons assume the episodes will be viewed as a class rather than individually. Before the lesson, you can check that all of the associated technology is working, and that the screen will be visible to all students.

## EPISODE CYBERSAFETY THEMES

---

Each episode deals with different, but related, cybersafety points. You may be able to add to the list of those identified.

### *Episode 2: Welcome to the Carnival*

- It is good to stop, and think for yourself, before acting.
- Young people need to check with a parent before accepting gifts.
- Bad websites can look like legitimate websites, and they can deliberately make 'terms and conditions' difficult to understand.
- There are several ways to judge if a website is legitimate. Legitimate sites will often have a prominently displayed privacy statement which explains how your personal information is handled. Good sites may also be ones that trusted adults know about and recommend for children to use.
- If something looks too good to be true, it probably is.
- Not every person you meet online is trustworthy.
- A wide range of people can access your details online – including people you might not want to have your personal information or people you hadn't anticipated.
- Young people can help other people by keeping an eye out for others online.
- Details like your name, address, school and your photo are unique and special to you. Ask a trusted adult before giving them out online.

### *Episode 3: It's a Serious Game*

- If something looks too good to be true, it probably is.
- Not everything in the online environment is true, or able to be trusted.
- Information online can be used in ways you don't intend.
- There are lots of scams online and scammers can misuse your information in multiple ways.
- Always check with a trusted adult (like a parent) before divulging your personal details online.
- It is okay to say no to any offer online that you have doubts about.
- There are lots of ways that unscrupulous sites try to trick you into giving them your information and many good ways to protect yourself.

### *Episode 4: The Info Gang*

- Some scams online may just be annoying, but some can actually harm you.
- Spam is email that you didn't ask for. Some spam can also be scams.
- Act on any doubts you have.
- If your personal information is online, it can sometimes be amended or deleted, but not always.
- People may use a range of methods in the online environment to try to elicit our personal information.
- If an online offer looks too good to be true, it probably is.
- It's ok to say no to any offer that you have doubts about.

### *Episode 5: Heroes*

- It's good to talk with a trusted adult about anything that upsets you online.
- You can help other people by keeping an eye out for others online.
- Good citizenship is important online and offline.
- Listen to your 'worried' uneasy feelings.
- The information you put online can reach a greater number of people faster than ever before.
- Stop and think before acting and remember to check with an adult first.

- While most activities online are legitimate, there are a few individuals intent on misuse—just as there are in the offline world.
- Sometimes people in the online environment will pretend to be someone or something you trust in order to try and get your personal information.
- Offers can come through mobile phones as well.
- Adults we trust in the offline world can help keep us safe in the online environment.

Teachers are welcome to develop their own lessons based around these and other cybersafety themes.