Fact sheet for parents:

Canvas (QLearn) Cyber incident

The department is aware of a global cyber security incident affecting the Canvas platform, the online learning system we know as QLearn.

The third-party provider Instructure has advised that the breach has been contained; however, there may be a range of educational institutions impacted worldwide.

We are working with Instructure and the Queensland Government Cyber Security Unit (QGCSU) to understand the scope of the incident and how department employees or students may be impacted.

It is important to note that QLearn remains safe to use.

The department's security protocols and monitoring activities have been intensified, as we determine the scope of the issue.

It is important for you and your child to be extra vigilant when it comes to your online behaviour.

Things to discuss with your child

- **Protect your personal information from scams** — Scammers use emails, text messages, or phone calls to convince you they are genuine and get you to share personal information, such as your address, to confirm your identity. Always verify a request for personal information with your school before providing any details. Refer to the safety

commissioner's tips for how your child can protect their personal identity online.

- **Do not click suspicious links and attachments** — explain to your child it is important they do not click links or download files unless they are confident they are from a trusted and verified source. Find more information about how you and your child can spot scams and suspicious links.
- **Limit sharing of personal information** — especially if you or your child are contacted unexpectedly or asked to verify details.

The following practices are recommended to help keep your child safe when they are online:

- Put computers in open spaces within your home
- Keep an eye on what your child is doing online (both in the home and on any mobile devices they have access to)
- Install software to limit their use and monitor/restrict the sites they visit
- Help your child to regularly update their privacy settings
- Teach your child how to create a strong password and have a routine for updating them
- Discuss a plan with your child about how to address any cybersafety issues that may arise (make sure they know you will be supportive if they mention anything and that they will not get in trouble).

Further information available for parents and children

The department's Cybersafety in Queensland schools page offers guidance to parents/carers on being safe online. The online awareness: Information for parents and caregivers (PDF, 726 KB) page provides important information for parents about cybersafety.

The e-Safety Commissioner also provides a suite of resources to support safer experiences online. There is a parent page which provides advice for parents and carers, as well as useful information to support young people protecting their identity online.

Supporting your child's wellbeing and mental health

We recognise that this information may be upsetting.

If your child is feeling worried or anxious about online risks, encourage them to speak to a trusted adult, such as a teacher, guidance officer or school wellbeing professional.

Ensuring the immediate safety and wellbeing of children is a priority.

Additional support is available through external organisations and resources.

- Lifeline—phone 13 11 14
- Kids Helpline—phone 1800 551 800 for free and confidential counselling for young people aged 5–25
- Parentline—phone 1300 301 300 for support, counselling and parent education
- Office of the eSafety Commissioner—parents and carers

Immediate response to online incidents

If your child has been targeted online, it's important to act quickly and calmly.

- Stay calm, encourage open communication and listen without judgement.
- Do not engage with the perpetrator. Advise your child not to respond to any messages, threats or demands such as sending money or images, as this can lead to further exploitation.
- Preserve evidence by taking screenshots and saving messages or emails.
- Report the incident using the o eSafety Commissioner's online reporting tool .
- Seek professional support if your child is distressed.

Reporting

Monitor your child's school account closely or any unusual activity and report anything suspicious to the Principal as soon as possible. If you have

concerns for your child's safety, report the incident to your local police. Phone Police Link on 131 444 or 000 if it is important to act promptly. Below are the steps you can follow to report cyber incidents and seek help:

1. If your child is in immediate danger or at risk of harm call **000** immediately.
2. Use the eSafety Commissioner's online reporting tool to report cyberbullying, image-based abuse, or harmful online content.
3. Australian Centre to Counter Child Exploitation (ACCCE) website to report child exploitation material or other criminal activities involving children.
4. Use the Australian Cyber Security Centre's ReportCyber tool to report cybercrime, such as online scams or fraud.