Digital Technology: Safe and responsible use in schools

The following guide is a companion to the Guidelines for the surrender and retention of property and searches.

Contents

Related downloads

- Digital technology: Safe and responsible use in schools [PDF, 2.5 MB]

Introduction

Education is changing. Digital technologies are everywhere and they are impacting what, where, how and why students learn, and who they learn from. Many schools are using digital technologies like the internet, laptops and tablets to quickly, easily and cost effectively connect students with the huge range of digital services and resources. However, the many benefits of learning with digital technologies are accompanied by some challenges and potential risks for students and schools. These 'digital challenges' are real and present a dilemma to schools seeking to use digital technology to enhance student learning.

Digital challenges can be broadly categorised as:

- **Cybersafety**: Involves conduct or behavioural concerns.

  Examples include cyberbullying, smear campaigns, accessing inappropriate content, creating spoof websites or sexting.

- **Cybercrime**: Involves illegal activity.

  Examples include sexual offending, accessing objectionable content or online fraud.

- **Cybersecurity**: Involves unauthorised access or attacks on a computer system.

  Examples include hacking into someone's social media service account, launching a Distributed Denial of Service (DDoS) attack or loading malware onto a laptop.

In general, preventative approaches that rely on technical or other protections simply do not work. These methods have a role but must be balanced with strategies that promote:

- development of skills and knowledge for safe and responsible use of digital technology
- opportunities for students to be involved in decisions about the management of digital technology at the school
- development of a pro-social culture of digital technology use, and
- cooperation of the whole community in preventing and responding to incidents.

The ultimate goal is to ensure the online safety of all students.

Purpose

The purpose of this guide is to support schools in the management of safe and responsible use of digital technology for learning. It is written within the context of:

the Sections (106 – 114) of the Education and Training Act 2020
Surrender, Retention, and Search Rules 2013; and

Guidelines for the surrender and retention of property and searches.

The aim is to provide principals and teachers with the information to act confidently and in the best interests of students with regard to digital technology.

Audience

This guide provides information about the safe and responsible use and management of digital technology for boards of trustees, principals and staff. It outlines key aspects of the context surrounding the effective management of digital technology in schools and kura. The explanations provided in this guide have been written to be as accessible as possible to a non-technical audience.

Contact

If you have any further questions arising from this guide, it is recommended that you contact NetSafe or the New Zealand School Trustees Association (NZSTA) for advice and guidance. They may be able to provide more detailed information about incident response and technical issues.

Contact details are:

NetSafe
0508 NETSAFE (0508 638 723) or queries@netsafe.org.nz

NZSTA
0800 782 435 or NZSTA website

Acknowledgements

We are indebted to NetSafe which has led the development of this guide on behalf of the Online Safety Advisory Group (OSAG). In particular, we wish to acknowledge NetSafe's consistent focus on the positive role that safe and responsible use of digital technology can have in student learning while providing practical advice on a range of complex issues that are challenging New Zealand schools and kura.

In addition, we are grateful for feedback from the Ministries of Education, and Justice, New Zealand Police, Education Review Office (ERO), Post-Primary Teachers' Association (PPTA), Secondary Principals' Association of New Zealand (SPANZ), Office of Children's Commissioner (OCC), New Zealand Association of Intermediate and Middle Schooling (NZAIMS), New Zealand Principals' Federation (NZPF), New Zealand Trustees Association (NZSTA) and Network for Learning Ltd. We also like to note the Office of the Privacy Commissioner's contribution and feedback.

This guide draws upon a range of reports, research articles and other resources. We acknowledge the contribution these materials and their authors make to this guide. References and links to these resources have been included in the Appendices section.

Online safety advisory group

Patrick Walsh, SPANZ, Chair
David Rutherford, HRC
Brian Coffey, MoE
Jan Breakwell, MoE
Phil Harding, NZPF
Denise Torrey, NZPF

Jenna Woolley, n4l
Lawrie Stewart, Police
Lorraine Kerr, NZSTA
Malcolm Luey, MoJ
Martin Henry, PPTA
Neil Melhuish, NetSafe
Roly Hermans, Police
Russell Wills, OCC
Paul Daley, SPANZ
Sandy Pasley, SPANZ
Stephanie Greaney, ERO
Suzanne Townsend, HRC
Wendy Esera, NZAIMS
Asad Abdullahi, MoE

Feedback

We welcome your feedback on all aspects of this guide at:
bullyingprevention@education.govt.nz.

SECTION ONE The guide at a glance

This section provides a summary of the guide's key points. It is recommended that this section is used as a companion to, not instead of, the rest of the guide.

In this section:

Understanding digital technology and information

Education is changing. Digital technologies are everywhere and they are impacting what, where, how and why students learn, and who they learn from.

Digital information is different from its physical counterpart in many ways. It can be rapidly duplicated, easily distributed and is able to be stored in multiple locations. These factors mean that it can be hard to control and completely eliminate.

Having an appreciation of these unique characteristics is key to developing an effective prevention and incident response plan. However, the effect is most keenly felt when a school needs to respond to an incident involving misuse of digital technology. School staff may feel that they do not have sufficient control over the digital technology involved to achieve a successful outcome.

The reality is, however, having greater control does not necessarily equate to a better outcome. Schools are advised to recognise and understand the nature of the changes and challenges that digital technology have brought and develop systems and processes to manage these.

Safe and responsible use of digital technology for learning

The overall objective for schools is to create a learning environment involving the safe and responsible use of digital technology. This is largely achieved by fostering a positive culture of digital technology use where challenges are understood to exist.

This approach should reduce negative outcomes by:

- reducing the incidents of misconduct involving digital technology
- minimising harm to students by effectively responding to incidents when they occur.

Prevention

Preventing incidents involving digital technology is better than having to respond to them. In general, prevention approaches that rely on technical protections, such as content filtering or activity logging, simply do not work. An effective prevention strategy is comprised of activities that are:

promotional: guiding young people's learning in the digital world, and
protective: mitigating or buffering risk by protection, support or intervention.[1]

Effective approaches to implementing safe and responsible educational use of technology are active and ongoing. They are underpinned by the idea that promoting safe and responsible use of digital technology is a shared responsibility.

Therefore effective communication between the school, teachers, students, parents and whānau about the role of digital technology in the life of the school and its wider community is central to an overall strategy.

[1] Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013)

Incident response

Even the most effective prevention programme will not entirely eliminate the risk of an incident occurring. It is critical that, as part of their prevention work, schools have developed and implemented a response plan before an incident occurs. The links between the prevention and incident response plans should be made explicit.

When things go wrong, the objective is to respond in a way that:

minimises student distress or harm
maintains student and staff safety i.e. does not make things worse.

There are two guiding principles for responding to incidents that schools need to consider:

Focus more on the behaviour involved in an incident, and less on the digital technology
Always act in a way that maintains the integrity of digital devices and the information stored on them.

The legislation and incident management

The Education and Training Act 2020 provides teachers and authorised staff with certain powers when they have reasonable grounds to believe that:

a student has digital information stored on their digital device or other digital technology that is endangering the emotional or physical safety of other students or detrimentally affecting the learning environment.

In relation to digital technology the term 'item' means either:

digital information comprising text, images, audio, video
digital devices such as a smartphone, laptop, camera etc.

Teachers and authorised staff **can** ask a student to:

reveal the item
delete the item
surrender the digital device on which the item is stored in
retain the surrendered digital device for a reasonable period.

Teachers and authorised staff **cannot**:

reveal an item on a digital device, or surrender the device without reasonable grounds
search through the content of students' digital devices or online accounts
ask for students' password access to the digital devices on which the item is stored
ask students to download or reveal what is on another digital device
use physical force against a student
ask two or more students to reveal or surrender their digital devices together without forming reasonable grounds in each case.

If a digital device is retained details of the incident must be recorded. If a criminal offence has occurred the device should be passed to the New Zealand Police at the earliest possible point; otherwise, at the end of the retaining period it must be returned to the person the item belongs to or the student's parents/caregivers.

Response planning

Identify the roles and responsibilities of internal staff and external organisations.
Identify and address any areas of crossover between the prevention and incident response approaches.
Develop and implement processes and procedures and then monitor them for consistency.

Schools' responsibility and authority to act

In general, a school's responsibility to maintain a safe educational environment justifies a measure of authority over off-premises and student after-hours conduct.
A school's focus should be on whether the misconduct has an adverse impact on the educational function of the school rather than when or where that misconduct took place.

Decisions about inappropriate and unlawful conduct

Identifying whether problematic conduct is inappropriate or unlawful will have a significant impact on a school's response. For example, if a criminally unlawful act has occurred, the Police should be contacted directly for advice

Identifying those involved in an incident

Identifying those involved in an incident is central to its effective management.
To help this process schools can:
make a record of all available information and seek specialist advice from NetSafe if required
look for relationships between online and offline behaviour including trying to identify digital bystanders to an incident.

Ownership of digital technology and information
School and student property are managed differently so a sound understanding of the ownership of digital technology and the content generated by students in curriculum delivery is necessary.
Generally, the devices in a Bring Your Own Device (BYOD) schemes are either the property of the student or the leasing company, not the school.
Generally, students own the copyright of any original work they create at school regardless of who owns the device it was created on.

Using social media and other online services in teaching and learning
Social media and other online services provide a range of tools that can be used to support innovative teaching practices and promote learning.
It is recommended that schools develop specific policies for the use of online services in teaching and learning. These could include:
account ownership
content ownership
privacy
guiding students' online behaviour

Surrender, deletion and retention

Surrender and retention

Searching for digital information is a specialist activity. The New Zealand Police are the only authorised agency to conduct such a search.
Teachers and authorised staff should not request any means of authentication that would enable access to the device or online service belonging to a student.
Storing a digital device involves both securing it physically and electronically.
Before handling a device it should, if it has the functionality, be locked by the student prior to them surrendering the device.

Requesting the deletion or surrender of digital information

A request made to a student for them to delete digital information from a device or website may not be effective.
Social media service providers will generally remove problematic content from their service depending on whether or not it has breached their Terms & Conditions. Schools can contact providers directly to request content removal but are advised to contact NetSafe first.
It is not possible to surrender digital information independently of a device.

Summary chart

SECTION TWO Understanding digital technology

This section explores the key characteristics of digital technology and the importance of understanding young people's online experiences and behaviour.

In this section:

Relevant characteristics of digital information

Digital information is very different from its physical counterpart. Physical information has a fixed position in place and time. This is not the case with digital information, which can be:

- **rapidly duplicated and easily distributed**
  e.g. a message posted via social media is reposted elsewhere by friends or an email sent to a list of recipients within a very short time frame
- **stored in multiple locations**
  e.g. a photo can be stored simultaneously on a laptop, a smartphone and in the Cloud
- **created and communicated automatically**
  e.g. a smartphone can synchronise emails with another device or an online service
- **stored with varying levels of 'discoverability'**
  e.g. image files that can only be accessed using a password or other method of authentication.

Digital information can be communicated rapidly

The 'viral' nature of digital communication enables information to spread rapidly and reach a wide audience. This can make it very difficult to know who has received the information or how it will spread further. It also requires any action to minimise harm that could be caused by this communication to be taken quickly.

Digital information is hard to permanently delete

Once digital information or items are created it can be difficult, if not impossible, to permanently delete all copies. For example digital information can be:

stored on a range of digital devices such as smartphones, laptops and internet servers as it is communicated. For example an email or chat message.copied and communicated automatically or to a schedule making it difficult to know what information is stored where. For example, a smartphone automatically synchronising stored information with a laptop computer or to the 'Cloud'.

retrieved or restored from the archive or trash after deletion using easily accessible tools.
temporarily stored on a device. For example, a device will download information to display a website and then can delete it when the web browser is closed.

Digital information can be remotely accessed

Typically, transmitting digital devices such as smartphones or laptops can be accessed remotely via another internet connection. Similarly, the content of a website can be remotely accessed and edited. Example of actions that can be carried out remotely include:

deleting, adding or editing information stored on a digital device or web page
accessing a device's location services to find its specific location, or
turning on a device's web camera and using it to record.

Understanding young people's digital and online behaviour

Understanding young people's digital experiences

Prevention strategies are effective when they reflect young people's understanding and use of digital technology.

Adults and young people participate in the online environment in very different ways. Their views also differ in the perception and management of online risks.

A study on the attitudes and behaviours of parents and teens in the United States of America (USA)[2] found that there is a 45% gap between the perceptions of these two groups when they were asked about how closely the parents were monitoring young people's online activities.

A significant number of young people do report negative experiences from the exposure to inappropriate content or harassment. For example, NetSafe research (2010) on young people's experience of digital challenge indicated that at the time just over half of them reported being targeted at least one instance of cyberbullying or harassing behaviour in the previous year. This was also the most distressing type of challenge they reported.

However, young people are also often able to merge prior knowledge with technical skill to develop cyber-risk management strategies.[3] They often choose to undertake risky practices because they believe the benefits outweigh the risks (i.e. cyber risk and resiliency is a developmental challenge and opportunity for young people).[4] Young people also have different levels of vulnerability to experiencing negative outcomes.[5]

The findings from a USA study on trends in youth internet victimisation[6] found between 2000 and 2010 that:

despite large increases in young people's online access their levels of online sexual victimisation had actually gone down over the time of the study. (19% in 2000 to 9% in 2010).
online harassment increased significantly (6% in 2000 to 11% in 2010).
reports of unwanted exposure to pornography over the same period was variable (25% in 2000, 34% in 2005 and 23% in 2010).

[2] The Family Online Safety Institute (2013)
[3] Hasebrink, Görzig, Haddon, Kalmus & Livingstone (2011)

[4] Byron (2008)

[5] Ringrose et al (2012)

[6] Jones, Mitchell & Finkelhor, D. (2012)

Online and offline behaviours are often closely related

Increasingly, young people's behaviour is a blend of online and offline experiences. For example, online and offline bullying or harassing behaviours are closely linked.

International findings showed that:

45% of youth who had been the target of online harassment knew the harasser in person before the incident and 25% reported an aggressive offline contact by the harasser[7]
those who are bullied offline are 15 times more likely to experience online bullying[8]
youth who are online victims may be online perpetrators as well.[9]

[7] Ybarra, M. L., Mitchell, K. J., Wolak, J., and Finkelhor, D. (2006)

[8] Hasebrink, U., Livingstone, S., & Haddon, L. (2008)

[9] Sourander, A. et al (2010)

Online identity can be different to offline

In the online environment, it can be quite acceptable to use a pseudonym instead of a real name. It is also possible to set up an online account by providing very little, or even false, information. Even when correct personal information is provided, it can be protected by privacy legislation or by the terms and conditions of use. Learning the identity of a person or persons behind an online identity can be, for practical purposes, impossible.

This means that it is easy to achieve a high level of anonymity or pseudonymity by using a false name to create a new persona or by co-opting someone else's identity. Online pseudonymity and anonymity can be used to change the balance of accepted power structures. This can be challenging for teachers whose authority can be easily undermined, for example, through the creation of a spoof website that is designed to attract negative comments from the school community.

SECTION THREE An overview of prevention and incident response

This section outlines strategies for preventing and responding to incidents in schools involving digital technology.

In this section:

Incident prevention

Prevention is better than response

Prevention is better than response

The characteristics of digital technology make it more important than ever for schools to work with their communities to prevent the likelihood of incidents occurring in the first place. Schools are encouraged to prioritise prevention activities and to make explicit links between these and their incident response plans. For example, prevention strategies aimed at understanding and 'breaking down' the school community's 'digital bystander' culture can also assist in the response to an incident.

Involving students, parents and whānau in meaningful discussions about the role of digital technology at school and beyond can help to prevent incidents occurring and reduce their impact when they do.

Balancing protective and promotional strategies

The key to effective prevention is to support the development of safe and responsible online behaviours. A deliberate, planned approach that balances protective approaches, such as technical mediation of student online access, with strategies that promote safe, responsible and pro-social behaviours is required. There are no quick fixes. A prevention strategy is ideally composed of a balance of activities that are:

promotional: resources and interventions that lead directly to healthy development; and
protective: when risk is mitigated or buffered by protection, support or intervention.[10]

10 Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013)

Guiding young people's learning in the digital world

NetSafe's 'Learn, Guide, Protect' model provides schools with a framework for structuring their prevention strategies around. It has three components:

> **Learn**: Students develop the competencies and values to keep themselves and others safe online. These are part of the broader concept of 'digital citizenship'.
> **Guide**: The programmes, practice and resources put in place to support student learning and develop a culture of positive digital technology at school and in the wider community. For example, integrating online safety into the school curriculum, developing teacher and leadership capability, strengthening relationships with family and whānau and engaging students in planning and delivery.
> **Protect**: Technical methods to restrict or monitor online access and school developed policies that underpin a safe and secure digital learning environment. For example, incident response plan and reporting channels, school policies and technical restrictions or monitoring of online access.

Active and ongoing risk management approaches

Effective approaches to implementing safe and responsible educational use of technology are underpinned by ongoing risk management processes.

An effective strategy could include initiatives such as:

implementing ongoing procedures for how digital technology is used at school. For example, by using Acceptable Use agreements and consent forms as living documents that are revisited during the school year.
developing a clear incident response plan for staff to follow that makes explicit links to prevention activities.
introducing a 'online safety or digital citizenship' theme across all school policies, processes and practices.

implementing processes to ensure that these policies are consistently applied.
developing communication channels that involve students, parents and whānau in discussions and decisions around online safety and digital citizenship. For example:
implementing an online safety or digital citizenship committee
creating a programme of training for staff, students and the community training to build whole school digital capability, or
creating opportunities for students to share their understanding of digital technology and challenges with adults and their peers.

Controlling student use of digital technology

Young people are accessing the internet with increasing frequency through a range of connection options. In addition to a school's network, students can get online via:

Cellular networks
e.g. a mobile data plan that gives access using a smartphone.
Community Wi-Fi
e.g. free or paid access to Wi-Fi using a laptop, tablet or other handheld device in a public space such as a café or library.
Home broadband
e.g. via multiple devices that include smart TVs and games consoles.

The range of available internet access points means that young people can potentially go online anywhere or at anytime using connections that may not be controlled by the school. This is just one way in which students can bypass technical protections designed to restrict or monitor their online access at school.

Effective prevention strategies emphasise approaches that actively involve discussing with students how they use digital technology, and more specifically, the challenges they experience online and how they can keep safe.

Involving the school community

It is recommended that schools actively engage with students, parents, family and whānau about the incident response plan, and seek their involvement in supporting the school's digital policies and procedures.

It is recommended that schools actively engage with their communities to help to:

create the idea that being safe and responsible online is a shared concern
support students transition between home and school digital technology use
reflect socio-cultural factors in the use of digital technology for teaching and learning
develop an understanding of how young people use the internet and the online challenges they experience
develop a positive culture of internet use where challenges are understood to exist and where mistakes are part of the learning process.

A starting point for developing a shared solution is to discuss how the school and its community envisage digital technology being used in the classroom and beyond.

Incident response

Planning and preparedness

Even the most effective prevention programme will not eliminate the risk of an incident occurring. It is critical that, as part of their prevention work, schools have a response plan in place before an incident occurs.

Prevention and incident response activities are linked. It is recommended that schools explicitly consider how their incident response plan complements their prevention work and vice versa.

Incident response objectives

Keeping safe and minimising harm

When responding to an incident, effective policies and processes will:

minimise student distress or harm
maintain student and staff safety.

Maintaining student safety and professional integrity are directly linked

How a teacher's actual, perceived or implied actions may be viewed later from an ethical or legal perspective is important in terms of maintaining their professional integrity whilst ensuring the safety of students.

Policies and professional practice should reflect an understanding of the special characteristics of digital technology and information. The general principle is that teachers and authorised staff act in a way that maintains the integrity of digital devices and the information stored on them i.e. to eliminate any possibility that changes can be made to the device or the information stored on it.

Focus more on behaviour, less on digital technology

The general principle is to focus more on the behaviour involved in an incident and less on the digital technology. Schools are not expected to be digital forensics experts and should use all other avenues of inquiry that are open to them. For example, as on and offline behaviours are closely related there is a high probability that a student who has been the target of online harassment will know the identity of the perpetrator. They are also likely to be experiencing offline, real world, harassment from the same person.

SECTION FOUR Responding to digital incidents

This section provides specific advice on how schools can respond to incident involving digital technology and also summarises the relevant legislation and rules governing what actions schools can take.

In this section:

The legislation and rules

The Education and Training Act 2020 and digital technology

The Education and Training Act 2020 contains provisions that are directly relevant to how schools should manage an incident involving digital technology when it is involved in an incident.

This advice is based on the Guidelines for the Surrender and Retention of Property and Searches and accompanying rules that the Secretary for Education released in January 2014.

The legislation provides teachers and authorised staff with certain powers when they have reasonable grounds to believe that:

a student has digital information stored on their digital device or other digital technology that Is endangering the emotional or physical safety of other students, or detrimentally affecting the learning environment.

What does the term 'item' mean in the legislation in relation to digital technology?

Digital information comprising one or more of the following elements:
text e.g. social media post, web page, email
image e.g. digital photo uploaded to the internet
audio e.g. music track, voice recording
video e.g. movie clip taken on a smartphone.
A digital device such as a smartphone, laptop, camera that can be used to create, edit, communicate, copy or store digital information.

What teachers can and cannot do

TEACHERS AND AUTHORISED STAFF CAN...	TEACHERS AND AUTHORISED STAFF CANNOT...

TEACHERS AND AUTHORISED STAFF CAN...	TEACHERS AND AUTHORISED STAFF CANNOT...
Ask a student to: reveal the item delete the item (if appropriate) surrender the digital device on which the item is stored retain the surrendered digital device for a reasonable period and while the item is in their possession, they must take all reasonable care of the item and if the device is to be retained for overnight or a longer period, it must be placed in secure storage. Teachers must ensure that a record is made and kept of the digital device. They have up to two days to complete this record. The record must show: the date on which the device was taken name of the student from whom the item was taken the name of the teacher or staff who took the device. At the end of the retaining period, the teachers must return the digital device to either: the student, or the person the item belongs to, or pass it on to the student's parents/caregivers. If a criminal offence has been suspected the device should be passed directly to the Police. For example in case of drug involvement, threatening to kill or do grievous bodily harm or criminal harassment.	Ask any student to reveal an item in his/her digital device, or surrender their digital device without forming a reasonable belief that the student's device is storing an item which is likely to endanger the emotional safety or detrimentally affect the learning environment. Search through the content of students' digital devices or online accounts. Ask for students' passwords to access the digital devices on which the item is stored. Ask students to download and/ or reveal items that are stored on another digital device, on a social media or other online service. Use physical force against a student. Ask two or more students to reveal or surrender their digital devices together without forming a reasonable belief that each student has an item that is likely to endanger the emotional safety or detrimentally affect the learning environment.

Summary chart: Surrender and retention of students' digital devices

This chart outlines a summary of the steps and processes in the legislation that deal with the surrender and retention of students' digital devices.

Key aspects of the legislation

Teachers must be familiar with the following aspects of the legislation which apply to the management of incidents involving students' inappropriate use of digital devices:

establishing reasonable grounds
revealing and surrendering
retaining and disposing of digital devices
refusal to reveal an item, produce or surrender digital devices
restrictions and limitations of teachers' powers
the complaints process.

Criteria – reasonable grounds

Section 106(1)(a)(b) of the Education and Training Act 2020 states:

(1) This section applies if a teacher or an authorised staff member has reasonable grounds to believe that a student has hidden or in clear view on or about the student's person, or in any bag or other container under the student's control, an item that is likely to:

(a) endanger the safety of any person; or
(b) detrimentally affect the learning environment.

Steps 1 and 2 on the chart summarise the criteria for requiring a student to:

produce an item i.e. a digital device such as a computer or mobile phone, or any other electronic device, or
reveal any information stored in digital form in a computer and other electronic devices.

A belief on reasonable grounds

Before acting under the legislation a teacher or authorised staff member is required to have reasonable grounds to believe that a student has hidden or in clear view on or about the student's person an item that is likely to detrimentally affect the learning environment or endanger safety.

The legislation defines an item in relation to the digital technology to be:

any tangible item such as a computer or mobile phone, or
any digital information stored on a computer and other electronic device.

A belief on reasonable grounds will depend on the circumstances and nature of the item and may also depend on other factors such as a student's age and maturity.

It is up to the teachers' professional judgement to decide if reasonable grounds exist for them to use their statutory powers to manage the incident at hand. For example, a smartphone is not in and of itself a danger to anyone or detrimentally affecting the learning environment. However, it could be used to send an inappropriate text or take a photo of students in the class without their consent. In this example the class teacher may have:

observed the student texting or taking photos, or
received that information from a reliable or credible source that a student misused an electronic device, or
a student who saw the text being sent or the students, whose photos were taken, complained to the teacher.

Then, the teacher would have a belief on reasonable grounds that the action of that student may be likely to detrimentally affect the learning environment or endanger student emotional or physical safety, depending on the nature of the text or the photos the student took of the unsuspecting students.

Revealing and surrendering

Section 106(3)(a)(b) of the Education and Training Act 2020 states:

(3) If the item is stored on a computer or other electronic device, the teacher or authorised staff member may require the student:

(a) to reveal the item:
(b) to surrender the computer or other electronic device on which the item is stored.

Steps 3, 4, 5 and 6 on the chart deal with the surrendering, retaining and/or disposing of digital device.

If reasonable grounds have been established a teacher can require a student to:

reveal digital items such as text or photos, or
surrender the smartphone on which the item is stored i.e. confiscating the phone from the student.

Revealing

The student must follow the teacher's instructions and reveal the text or photos to the teacher while still in possession of the device or other technology. A teacher cannot search the digital device.

As part of investigating the incident, the teacher may need to find out from the student whether they have shared the text or photos with anyone else (in the class or outside of the class), or have stored them in any other digital device including servers in 'the Cloud'.

The teacher's decision-making process about whether to request that item to be revealed will be guided by factors that are relevant to the case. These may include:

the nature of the text or photos
whether the student has shared the photos by sending them to other students
the attitude and the emotional impact on the affected students
the student's age and maturity, and
any other relevant factors.

Viewing the item requested could also indicate that there are other items of concern on the phone. Teachers can ask the student to reveal such items. Also teachers may form a reasonable belief about the existence of other devices in the control of other students and this may lead them to separately ask each of these students to reveal items on their phones.

Teachers cannot request that a student use one digital device to access information stored another digital device, such as website content stored on internet servers, to which the phone may be linked and which may be accessible from that phone. This means that teachers cannot ask a student to download or reveal information that is stored in any of their online accounts, such as for a social media site or online Cloud storage service.

Teachers must be satisfied that there is a reasonable belief that the student has the item stored on the computer or device under his/her control before they act under the legislation. The item must be on the device in order to be requested. It cannot be requested for an item to be added to a device from elsewhere for viewing, for example, asking for it to be downloaded from the internet.

Surrendering

After the teacher has had an opportunity to view the text or the photos he/she may be able to establish the scope and nature of the issue. This will inform the subsequent action required.

One option is to request the surrender of the digital technology. This action should be reserved for situations where there are reasonable concerns that the data on the digital device is harmful and the device needs to be retained for further investigation or preventing harm to occur. Teachers should avoid using the surrender of electronic devices as a punishment.

Note that it is not possible to surrender digital information independently of the device it is stored on. This would create more copies of the information. If the digital information is stored on the internet it also isn't technically possible to request its surrender. In this case, a surrendered device will, at best, contain a copy of the information that has been revealed.

Retaining and disposing

Section 106(4)(a)(b) of the Education and Training Act 2020 states:

(4) A teacher or an authorised staff member may do either or both of the following to an item surrendered under this section:

(a) retain the item for a reasonable period.
(b) dispose of the item.

In this example, the teacher may retain the surrendered smartphone for a reasonable period.

Rules 6 and 10 of the Education (Surrender, Retention, and Search) Rules 2013 state:

6 Considerations to be taken into account in dealing with **items or devices taken under Act**

(1) A person must take into account the considerations specified in subclause (2) when the person decides, under the Act or these rules, whether—

(a) an item or a device taken under the Act is to be retained, returned to a student, passed to another person, or passed to another agency; or
(b) an item taken under the Act is to be disposed of.

(2) The considerations are—

(a) the health and safety of people:
(b) the apparent value of the item or device concerned:
(c) the person believed to be entitled to the possession of the item or device concerned.

10 Record of retentions

(1) Each board must ensure that a record is made and kept of every item or device taken under the Act that is retained—

(a) for 2 nights, each of which follows a day on which the school is open for instruction; or
(b) for a longer period.

(2) Every record must contain the particulars that the board prescribes from time to time, which must include the following:

(a) the date on which the item or device was taken:
(b) the name of the student from whom the item or device was taken:
(c) the name of the teacher or authorised staff member who took the item or device

Section 106(5)(6)(7) of the Education and Training Act 2020 states:

(5) A teacher or an authorised staff member may retain a computer or other electronic device surrendered under subsection (3)(b) for a reasonable period.
(6) If an item or a computer or other electronic device is retained under this section, it must be stored in an appropriate manner.
(7) At the end of any period of retention, any computer or other electronic device, or any item that is not disposed of under subsection (4)(b), must be —

(a) returned to the student; or

(b) passed to another person or agency, as appropriate.

Under this section, it becomes the teacher's responsibility to appropriately store and look after any digital devices that students have surrendered to them.

Rule 7 of the Education (Surrender, Retention, and Search) Rules 2013 states:

7 Retention and storage of items or devices taken under Act

(1) This rule applies to any item or device that has been taken under the Act and is to be retained.
(2) Every teacher and every authorised staff member who is in possession of the item or device must take all reasonable care of the item or device while it is in his or her possession or under his or her control.
(3) The teacher or authorised staff member who takes the item or device may—

(a) keep the item or device in his or her possession; or
(b) give the item or device to another teacher or to another authorised staff member; or
(c) arrange for the item or device to be placed in secure storage.

(4) A teacher or other staff member of a school who is in possession of an item or a device that is to be retained overnight or for a longer period must ensure that the item or device is placed in secure storage.

A device that has been surrendered because of criminal activity should be retained only until it is practicable to pass it onto the Police.

At the end of the retention period, teachers may return the digital device to the student or pass it on to parents. Teachers should avoid using the retention or destruction (disposal) of electronic devices as a punishment.

Teachers are permitted to request the deletion (disposal) of digital information. Before doing so they should be satisfied that this request will achieve the desired outcome. For example, there may be multiple copies of the information, or it may be required as part of an investigation.

Refusal to reveal items, produce or surrender digital devices

Section 111(1) of the Education and Training Act 2020 states:

If a student refuses to reveal, produce, or surrender an item or computer or other electronic device under section 106(2) or (3), a teacher or an authorised staff member may take any disciplinary steps, or steps to manage the student's behaviour, that the teacher or authorised staff member considers reasonable.

If a student refuses to follow teachers' instructions to either reveal an item on a digital device or surrender the digital device itself, then, the student can be disciplined in the usual manner for any breach of school rules.

Restrictions and limitations placed on teachers' powers

Section 109 of the Education and Training Act 2020 states:

(1) Nothing in section 106 or 107 permits a teacher or staff member—

(a) to search any student; or
(b) to use physical force against a student; or

(c) to require a student to provide a bodily sample (but a teacher or staff member may encourage a student to participate in a voluntary drug treatment programme that involves testing of bodily samples).

(2) Nothing in section 106 or 107 permits a teacher or an authorised staff member to have a dog with him or her for the purpose of exercising a power under that section.

(3) The powers set out in sections 106 and 107 may not be exercised in relation to 2 or more students together unless the teacher or authorised staff member has reasonable grounds to believe that each student has an item specified in section 106(1) or a harmful item on or about his or her person, or in any bag or other container under his or her control.

The following restrictions apply to teachers when managing an incident involving students' digital devices. Teachers are not allowed to:

ask any student to reveal an item in his/her digital device, or surrender their digital device without forming a reasonable belief that the student's device is storing an item which is likely to endanger the physical or emotional safety or detrimentally affecting the learning environment
search through the content of student's digital devices
ask for students' passwords to access the digital devices on which the item is stored
ask students to download or reveal what is on other digital device for example, from student's social media or online account or in the Cloud
use physical force against a student
ask two or more students together to reveal or surrender their digital devices without forming a reasonable belief that each student has an item that is likely to endanger physical or emotional safety or detrimentally affecting the learning environment.

The management of an incident involving student's digital technology should be carried out:

in a manner that gives the student the greatest degree of privacy and dignity
away from the view of other students.

Complaints process

Parents'/caregivers' complaints about the way a school managed an incident involving digital devices in relation to its policy on the surrender and retention of student property should be dealt with through the normal school complaints procedure.

Roles and responsibilities

Planning a response

Consider the following with regards to the roles and responsibilities of internal staff and external organisations.

Internally

Identify existing internal expertise and plan for ongoing professional development.
Designate responsibility for developing incident management policies and processes.
Create an online safety group or digital citizenship committee that includes young people and community members to advise on prevention and incident response.

Externally

Include contact with the following external organisations in the incident response plan.
New Zealand Schools Trustees Association (NZSTA) provides services to support its members in their governance and employer roles.
NetSafe provides content and services to support schools to manage incidents. Plan to contact them early in an incident for specialist advice.
NZ Police – The Lead Police Contact is the conduit to the relevant police group for incidents in which a crime may have occurred.
Other key community organisations such as church groups, marae, youth or sports clubs.

Schools' responsibility and authority to act

Schools are involved in an increasing number of incidents where the activities of students at home or in their own time have an impact on the life of the school. This presents teachers with the challenge of knowing the extent of school's power and responsibility to act in such cases.

When an incident comes to the attention of the school, it can be difficult, if not impossible to establish when or where misconduct involving digital technology first took place. In general, a school's responsibility to maintain a safe educational environment justifies a measure of authority over off-premises and student afterhours conduct. When establishing a school's power and responsibility to act, a school's focus should be on whether the misconduct has an adverse impact on the educational function of the school rather than when or where that misconduct took place.

Regardless of whether a student has created inappropriate digital content on their own digital technology or away from school or not, schools have the responsibility and the power to act when any such content could reasonably be expected to impact negatively on the school learning environment.

Distinguishing between inappropriate and unlawful conduct

Inappropriate and unlawful conduct can be broadly divided into two areas: conduct that can be addressed through criminal law (i.e. a criminal offence), and conduct that can be addressed through civil law. General information on types of problematic conduct and relevant legislation is provided in the Appendices.

Identifying those involved in an incident

Identifying those involved in an incident is central to its effective management. This can be hard to do using the digital technology involved and schools should use a range of enquiries. In general, there are three roles in incidents involving the misuse of digital technology:

- perpetrators
- targets
- bystanders.

The relationships within and between these categories can quickly become complex, for example, targets and bystanders can also be perpetrators. It is recommended that schools:

make a record of all available information

While the identity of those behind a webpage or communication may be anonymous, it is important to collect all available information

before it is changed, removed or hidden. Schools should consider seeking specialist advice.

look for relationships between online and offline behaviour

Young people who have been the target of online harassment often know the perpetrator in person before the incident. They are also likely to be experiencing offline harassment as well.

be aware of the central role of bystanders

In psychology the 'bystander effect' refers to the phenomenon in which the greater the numbers of people present, the less likely people are to help a person in distress. In the majority of online incidents, there will be digital bystanders, whose role may be either passive or active. For young people, the culture driving bystander behaviour is strongly related to peer relationships. Understanding and 'breaking down' a bystander culture is both a prevention and response activity.

Ownership and digital technology

Identify who digital technology belongs to

Schools need to have a sound understanding of the ownership of digital technology and the content generated by students in curriculum delivery.

It is recommended that issues relating to ownership be specifically referred to in school policies, including User Agreement Policies (UAP). Note that it is not possible to use such policies to waive rights afforded to students by the Education and Training Act 2020, New Zealand Bill of Rights Act 1990 (BORA) or any other New Zealand legislation.

Ownership in 'Bring Your Own Device' schemes

Schools are adopting Bring Your Own Device (BYOD) schemes to increase the digital technology available for student use at school.

Typically BYOD ownership models involve devices being either:

purchased by parents and whānau
leased to parents and whānau through a master lease agreement held by the school, or
directly leased by parents and whānau.

In all cases, the devices are either the property of the student or the leasing company, not the school. School policies and practices should reflect this.

Ownership of online content and communications

In general, students own the copyright of any original work they create at school regardless of who owns the device it was created on.

Using online services in teaching and learning

Social media and other online services provide a range of tools that can be used to support innovative teaching practices and promote learning. It is recommended that schools specifically address the use of such services for teaching and learning as part of their broader policy development process.

As a general principle, schools should have an understanding of the Terms & Conditions (Ts&Cs) for services that they recommend for use in teaching and learning. For example, social media services typically require users to be a minimum of 13-years-old, although it is not a legal requirement in New Zealand. Note that as each service is different it may be necessary to seek specific advice and guidance in each case.

Accessing student accounts

Accessing a student's online account constitutes a search and is not permissible under the Education and Training Act 2020. In addition, account holders will be in breach of a service's Ts&Cs if they disclose their login details or let anyone else access their account.

Requests for students to reveal the content of their account should be made in such a way that it cannot be construed as a search. Such a request should only be made when the conditions of the legislation are met and should not cause the student to breach any terms or conditions of use.

Giving permission to use online content

Typically, content uploaded to a social media service belongs to the person who opened the account used to upload information. A social media provider may, however, apply Ts&Cs that enable them to use uploaded information for their own purposes, sometimes in perpetuity, even after information or an account has been deleted by the account owner.

Developing policy for using online service in teaching and learning

It is recommended that schools consider the following.

Account ownership

Ensure that each student or parent has his or her own account.
Discourage the practice of sharing account logon details.
Ensure that the students are above the minimum allowable age for account holders.
Set appropriate boundaries for how an account is used for personal and school use. Encourage students to think about appropriate online behaviour and managing their online profiles.

Content ownership

Make sure there is a clear understanding of the rights of service providers over uploaded content. Decide if this is acceptable in the context of the planned activities.

Privacy

Encourage students to think about their online privacy. For example, ensure students:
understand what constitutes personally identifying information, and what information is visible and to whom
have an understanding of the way information may be used
have an understanding of who may have access their information, now and in the future.
Provide guidance about the appropriate level for privacy settings. i.e. Is information being shared between classmates, with families

and whānau or will it be available on the web for anyone to find and view?
Will private information be shared with third parties such as advertisers?
Decide if this is acceptable in the context of the planned activities.
Ensure compliance with the service provider's policies relating to privacy, trust and safety.

Guiding

Develop specific policies on:
communication with and the involvement of families, whānau and the wider community
online relationships between staff and students.
How the internet will used in prevention and incident response activities. For example, consider:
creating a school social media presence that encourages participation of students, parents and whānau
how to use the internet positively when responding to an incident.

Searching for digital information

Under the Education and Training Act 2020, teachers and authorised staff are not permitted to search a student's digital device or online account for information, because doing so will breach students' rights to privacy. There are other good reasons for schools to avoid taking this course of action. Conducting a search for digital information not only compromises students' rights to privacy, but is a specialist activity.

The New Zealand Police are the only agency authorised to conduct such a search and they would follow their own processes as required by the situation. While specialist forensics service providers can conduct a search, schools do not have the authority to enlist their services to conduct a search of a student's digital technology.

Why searching is not a practical solution

Maintaining the integrity of stored digital information

The action of searching can change the information stored on the device. Digital technologies typically make a log of the actions carried out. Any attempt to access a device to conduct a search will be recorded, potentially compromising student safety and teachers' professional integrity. Teachers accessing a student's digital device may:

open themselves up to the accusation of having tampered with the device or information stored on it
break a chain of evidence that could be used to prevent harm being caused to a student or in disciplinary and law enforcement processes, or
infringe the privacy rights of other people who may have information stored on a device, such as parents.

Carrying out a focused search

Specialist knowledge and tools are required to carry out a focused search as opposed to 'trawling' through information stored on a device. The information being searched for may be:

a small part of a vast collection of text, images, audio, video and other data
inaccessible because it is protected by authentication or encryption
not stored on the device because it has been deleted or never existed.

Handling digital technology

Develop consistent practice across the school

It is recommended that consistent standards and processes be applied to the surrender and retention of digital technology. This eliminates the opportunity for later disputes about tampering, changing settings, accidental damage and use of bandwidth or privacy infringements.

Maintain the integrity of digital information

Storing a digital device involves securing it physically and electronically to ensure that the device itself is not physically lost, stolen or damaged; and that the digital information on the device is not remotely accessible. This prevents the information from being accidentally or intentionally changed.

For devices that can connect to a network (e.g. via 3G, 4G, Wi-Fi or Bluetooth) such as laptops, tablets or smartphones, the aim is to block the device from sending or receiving signals. This can be achieved by simply turning the device off or switching it to 'flight mode'.

The student should also lock the device before surrendering it. A locked device can only be accessed using a PIN, password, fingerprint or other means of personal authentication. This action eliminates any question of whether the school has access to the device while it is in its possession. It is also appropriate to turn off or lock non transmitting devices (i.e. those that cannot connect to the internet or other network) if possible before storing them.

Teachers and authorised staff should not request any means of authentication that would enable access to the device or online service belonging to a student. This action protects the student and the teacher.

Developing a policy for handling digital devices

Consider the following questions when formulating school policy for the surrender, retention and storage of digital technology:

Surrender

How will the surrender of a device contribute to resolving the incident?

Is the digital information actually stored on this device?
Are there copies elsewhere?
Is specialist advice needed before the request is made for a device to be surrendered? Is this expertise available internally?

Retention

Who owns the device? Does it belong to the student, school or a third party?
Will the device be needed as evidence, for example, to discuss with parents, senior management or the police?

Storage

Before storage, has the device been:
locked by a PIN, password or other means of authentication?
isolated from any external connection by being switched off or turned to 'flight mode'?
A record should be made of:
the incident and reason for requesting the surrender of the device
the time and place of the device's surrender
action taken to secure the device prior to storage
staff and students involved in the incident
planned follow up action.
Factors that schools should consider when retaining a device include whether it is:
used for maintaining the health and safety of the student
used for learning
implicated in an incident and the severity of that incident. For example, involving unlawful behaviour.

Removing problematic digital information

Delete only when it is appropriate

Prompt action can help to prevent problematic content spreading and can be effective approach in reducing any distress or harm that may be caused. Responding quickly is a key factor in achieving a positive outcome. However, digital information can only be deleted with complete confidence if all copies are removed and cannot be restored or accessed from another source. A request for digital information to be deleted should only be made with:

a clear understanding of what this action is aiming to achieve and its likely success
the knowledge that this action could break or add the school to the chain of evidence.

Assessing whether to request deletion of digital information involves asking questions such as:

What is the problem we are trying to solve? Will this action achieve the required result? What other courses of action could help to solve this problem?
Is the digital information unlawful or inappropriate? Will the information be needed later as evidence, for example, to discuss with parents, senior management or the police?
What type of digital information is causing the problem? Is it an image, movie or text?
Who owns the information? Who has access to it?
Does a third party need to facilitate deletion of the information, for example, a social media service provider?
Is external advice needed from NetSafe on the appropriateness and likely success of the request for deletion?

If deletion is the appropriate response:

Is the device connected to the internet? Has the information already been communicated? If so, how and where?
Where is the information stored? Is it on a device or is it website content? Is a password required to access the information?
How many other locations might it need to be deleted from? Are they accessible?
What assurances are there that the item is deleted and cannot be restored later?

Is external advice needed from NetSafe to assist in facilitating the uncontested removal of online content?

Removing problematic content from social media and other online services

Increasingly, incidents challenging schools involve content or communications that have been uploaded to a social media or other online service. These can be inappropriate or potentially unlawful. The removal of this content can have an immediate and positive impact on those targeted. In the majority of incidents, the target may already know the perpetrator. This means that there is a high probability that the identity of the perpetrator is discoverable. If their identity is known, the person who posted it could be asked to remove the content.

The majority of social media and online service providers are located overseas and not subject to New Zealand law. However, they can remove content from their services on the basis of whether or not it has breached their Ts&Cs. Schools can contact providers directly to request content removal by using a service's reporting functions. However, before doing so, schools should contact NetSafe for advice on the best course of action.

NetSafe has:

expertise in resolving incidents involving inappropriate or unlawful online content and communications
specialist knowledge of social media services' Ts&Cs
established working relationships with many of the leading social media and other online service providers.

NetSafe can advise schools on the likely success of content removal requests and, where appropriate, can act as an intermediary to facilitate such requests. This can usually be achieved in much shorter timeframes than schools can achieve through a direct request to the service provider.

SECTION FIVE Scenarios

This section presents a range of potential digital incident scenarios and explores how schools can respond in such situations.

The scenarios are based on actual incidents that have taken place in New Zealand schools and kura.

In this section:

1. Intimate photos taken with a smartphone

Students 'A' and 'B' were in a relationship that ended acrimoniously. Student 'A' complained to the Dean that Student 'B' had some intimate photos of her on his smartphone, which he had threatened to send to others. Student 'A' was distraught and asked

the Dean to confiscate Student 'B''s phone and delete the photos.

Incident response

Is unlawful conduct involved?

Depending on the context surrounding this incident an unlawful act may have already taken place. For example were the images:

taken covertly by Student 'B' i.e. without Student 'A''s knowledge or consent?
being used to intimidate, threaten or harass Student 'A'?
obtained through coercion or through other predatory behaviour?

If it is believed that a criminal offence has occurred referring this matter to the Police is the appropriate course of action. Prior to handing a device to the Police, ensure that it is managed in an electronically secure way.

If the images were published as threatened by Student 'B', this action could either be an infringement of civil law (e.g. Student 'A' could own the copyright of the images or have their privacy invaded by this action) or a criminal offence (e.g. if Student 'A' was a child).

Depending on the context, there could also be other problematic online or offline behaviours such as the threat of, or actual, physical harm. If the school has reason to believe that a criminally unlawful act has occurred the Police should be contacted directly for advice. For infringements of civil law the school should follow its relevant policies.

Does the Education and Training Act 2020 apply to this scenario?

Regardless of whether unlawful conduct is involved; the reported behaviour of Student 'B' was inappropriate and it has had an immediate impact on the emotional safety of a student and possibly the school's wider learning environment. The school can respond to the threat to publish the images on the basis that, if carried out, this will have a potentially harmful effect on Student 'A'. The primary goal for the school is to prevent the images from being published online, as this future action would impact on Student 'A'.

Is confiscation (surrender) of the device an appropriate course of action?

Surrender and retainment of the device are appropriate actions in this scenario, primarily because there is good reason to believe that the phone provides a channel for publishing the images. The images may already have been copied to another device or uploaded to the internet, perhaps to a file storage website.

Is deletion an appropriate course of action?

Key questions that will inform schools whether requesting the deletion of the images is appropriate are: "If it were possible, would the act of deleting the images in and of itself resolve the issue and minimise the harm?" and "Will deleting images from the phone prevent the images from being published at some point in the future?" The most likely answers to these questions are "no" and "possibly".

An effective solution will have a strong focus on Student 'B''s behaviour. For example, does Student 'B' understand that 'trust in a relationship' is a principle recognised in civil and criminal law i.e. that such intimate images need to be treated appropriately during and after the relationship ends

Questions and comments

Is this inappropriate or unlawful conduct? Factors to consider include:

Are the images objectionable material? Refer to page 45 for definition.

Is age an important factor in this incident? For example, the images could constitute objectionable material, depending on the age of Student 'A'. Is Student 'B' an adult and Student 'A' a child?

Were the images taken covertly, without the knowledge or consent of the person? (Note that images taken with legal consent are not covered by law)

Is there an element of coercion? For example, blackmail for more images, images of friends or money?

Is there an element of threatening, intimidating or harassing behaviour relating to physical harm to person or property (as defined by the law)?

Did Student 'A' take the original image? If so, Student 'A' owns the copyright and permission would be required from Student 'A' for the images to be published.

The phone and the images are important, but the primary focus is on student behaviour.

The threat to publish the images is clear, but is it an isolated event? What is the wider context of this incident? Has the dispute between the students been ongoing and, if so, how has this manifested itself? Is the whole problem understood?

Student 'B' has been identified by Student 'A', meaning that online anonymity is obviously not an issue. Both students can be easily interviewed, and, if required, their parents/caregivers contacted.

Even though Student 'B' is easily identified, consider that there are likely to be 'bystanders' to this incident. Is it useful to locate them? If so, how?

Is deletion an appropriate response to resolving the issue? For example, deletion from the phone may not achieve the desired result. To successfully delete all copies requires knowing and accessing all places it is stored.

If a school is overtaken by events and the images are posted online, a request can be made to the hosting service for them to be removed. Seek advice from NetSafe on this.

2. Video recording of an alleged assault

Students 'A' and 'B' were at a party and there was an incident following which Student 'A' has claimed an assault on her by Student 'B'. Student 'A' says it was recorded by Student 'C' on his smartphone. Student 'A' has complained to the Deputy Principal about Student 'B' and wants the school to confiscate Student 'C''s phone as evidence.

Incident response

Focus more on behaviour, less on digital technology

Although the alleged incident occurred off-premises and after-hours, when establishing a school's power and responsibility to act, the question is not where or when misconduct took place but what the impact is on the school or its students.

Further, the focus should be first on the behaviour and not the digital technology. Once the school becomes aware of an alleged assault, it has a clear duty to act and the matter should be referred to the Police.

The role of digital technology

The possible existence of a recording of the incident means that there is the potential for:

endangerment of student safety i.e. by posing an immediate threat to the physical or emotional safety of a person

detrimental affect on the learning environment i.e. disrupting the school environment through gossip, innuendo and intrigue.

The recording taken by Student 'C' of the alleged assault poses an immediate threat should they decide to share it. The recording could also provide direct evidence useful to the investigation of the incident. These arguments provide the Deputy Principal with a firm basis for a decision to take action in this incident. A request for Student 'C' to surrender the phone can be made. The device should be electronically and physically secured, and provided to the Police as soon as practicably possible.

In its investigation, the school should also seek to discover how far the images might have spread. For example:

have any copies of the images been made?
have they been communicated to a third party and, if so, how?
have they been posted online and, if so, where?

3. Pornography on a school laptop

Student 'A' was using a school laptop in the library and invited a group of friends to look at a website with pornographic and violent images. Another student viewing it was very disturbed by the content and told the librarian the laptop should be confiscated and examined.

Incident response

The laptop is the school's property and the teacher can ask the student to surrender and search the device. Schools may wish to consider the following issues and questions:

How have the images been accessed? This will inform the school as to whether they only need to focus on the laptop, or whether images could be on other devices or their servers.
Were the images:
loaded to the laptop locally. For example, using a USB memory stick?
accessed via the school's network?
accessed using the student's own internet connection (e.g. via a tethered mobile device) or a third party connection (e.g. community Wi-Fi)?
If accessed via the school's network, were any security and content filtering systems bypassed e.g. using a Virtual Private Network (VPN)? Whose network account was used?
What type of images are involved? Are they inappropriate (i.e. restricted) or illegal (i.e. objectionable material)?
Were the images being viewed illegal content? If so, the laptop should be secured electronically and physically and the incident reported to the Department of Internal Affairs.
If the images were inappropriate, could they become evidence in a school-based discipline procedure? If so, the laptop should be secured electronically and physically and an examination conducted by a digital forensics specialist on behalf of the school board.
Will a review of the school's prevention strategies be carried out after this incident? For example, are the school's policies on appropriate use of digital technology clearly stated and understood by students? What pastoral support is in place for students witnessing the content?

4. Using instant messaging to organise a fight

Student 'A' and his friends have decided to settle their differences with Student 'B' and his friends from another school. He has sent text messages to his friends and Student 'B' saying they need to meet in a local park to have a fight to sort things out. The Deputy Principal hears a rumour about the proposed fight but is unsure where it will be or when. No one is talking, but he believes the information is on Student 'A''s phone.

Incident response

In this scenario, the Deputy Principal has reasonable grounds to believe that the text messages are being used to create a situation that could:

endanger student safety i.e. by posing an immediate threat to the physical or emotional safety of a person
detrimentally affect the learning environment i.e. disrupting the school environment through gossip, innuendo and intrigue.

The Deputy Principal could consider the following:

It is possible that a criminal offence has already been committed or could be if a fight occurs. If the situation warrants, a decision may be made to contact the Police.
Text messages can be sent in a range of ways, some may involve the message being automatically deleted by the phone.
There are no technical methods that can confirm that the rumoured text messages exist, as a search of the device is not permitted.[11]

How much time should be spent focusing on investigating the text messages? Approaches that seek to break through the 'bystander effect' are likely to be more effective. However:

student 'A' can be asked to reveal the text messages. If they refuse they are subject to the school's disciplinary procedures.
if text messages have been sent by Student 'A' other people may also have a copy. If there are reasonable grounds, a request can be made for them to reveal text messages received from Student 'A'.

[11] Note that even if it were permitted, it would need to be carried out by a specialist and this process would take too long to help in this incident. Time is of the essence.

5. Recording an incident in the classroom

A teacher had an unruly class on Monday where there was a strong exchange between him and some students, this included a student swearing and storming out of class. The teacher discovered that a student recorded this incident on his smartphone and intends to upload the video to the web as a joke. The teacher wants the phone confiscated and the content deleted as he considers it would be humiliating and an invasion of privacy for all concerned.

Incident response

Has there been an infringement of the Privacy Act 2020?

Individual students are subject to the Privacy Act 2020 (the Act) as it applies to "any person or body of persons, whether corporate or unincorporated".

In relation to the Act, incidents involving digital information stored on a smartphone or other mobile device should be considered on a case-by-case basis. There is a range of factors to consider such as the applicable privacy principles and any exceptions to the principles or the Act itself. The general advice is to refer to the board of trustees' privacy policy in relation to the Act and seek specialist advice if required.

Again, in relation to this specific case the board of trustees' privacy policy should guide the process that the school follows.

What other options are open to the school?

The threatened action of publishing the video online, or otherwise sharing the recording, has the potential to:

detrimentally affect the learning environment i.e. disrupting the school environment through gossip, innuendo and intrigue
endanger teacher safety i.e. be harmful by posing an immediate threat to the emotional safety of a person.

This gives the school the basis to act in this case. The advice on deletion provided in this guide applies in this case.

SECTION SIX Appendices

This section contains a range of information about the organisations, online resources and support that schools can access to further build their knowledge and capability in this area. It also provides general information on problematic conduct in the context of relevant criminal offences and civil law.

In this section:

Support Resources

Key contacts

New Zealand School Trustees Association (NZSTA)

Phone: 0800 782 435 (STA HELP) toll free from anywhere in New Zealand

NetSafe

Phone: 0508 NETSAFE (638 723) toll free from anywhere in New Zealand
Email: queries@netsafe.org.nz

Police

Your school's Lead Police Contact is the conduit to the relevant Police group, if you think that a crime has occurred.

Contacts for your local police station(external link).

Refer to the Police's engagement model(external link) used to guide the development of their relationships with schools.

Privacy Commission

The Privacy Commissioner administers the Privacy Act 2020. The Privacy Act applies to almost every person, business or organisation in New Zealand.

Phone: 0800 803 909 toll free from anywhere in New Zealand
Email: enquiries@privacy.org.nz

The Commissioner can investigate complaints about actions that may be a breach of the privacy principles in the Privacy Act. They can also consider matters that may breach other provisions of the Privacy Act.

More information on complaints(external link).

Incident reporting

Telephone crime reporting

Crimestoppers provides an anonymous telephone reporting service.
Phone: 0800 555 111

Online crime reporting

The ORB(external link) offers all New Zealanders a simple and secure way to report their concerns about online incidents.

The ORB's partners currently include: NetSafe, Police, Department of Internal Affairs, Privacy Commissioner, Consumer Affairs, Commerce Commission, National Cyber Security Centre and the New Zealand Customs Service.

Report to NetSafe through Pond

Pond is the Network for Learning portal. It is an online environment uniting New Zealand teachers and school administrators with providers of educational content and services.

Pond's homepage(external link) provides a simple and secure way for authenticated Pond users to report directly to NetSafe any online content, communication or other behaviour that you think may be inappropriate or unlawful.

Support | Help and guidance resources

Related Reading
Bullying prevention and response: A guide for schools, Ministry of Education (2014)
Guidelines for the surrender and retention of property and searches, Ministry of Education (2014)(external link)
Privacy in Schools: A guide to the Privacy Act for principals, teachers and boards of trustees(external link), Privacy Commissioner(2009)

Developing school capability

Other resources to support professional discussions about how to develop the safe and responsible use of technologies.

NetSafe Kit for Schools, Version 4(external link) (2013)
e-Learning Planning Framework, Ministry of Education (2014)
Māori medium e-Learning Planning Framework Te Rangitukutuku, Ministry of Education (2013)
OWLS. An online privacy resource for younger children(external link) (2013)

Online service support

In partnership with a range of online service providers, NetSafe has produced a guide of practical tips called 'Staying Safe: Cybersafety tips from NZ's leading online companies'.

Direct links to providers' support resources:

Facebook(external link)
Google(external link)
Yahoo!(external link)
Microsoft(external link)
Trade Me(external link)

Criminal offences and civil law

General information on types of problematic conduct and relevant legislation is provided below. This does not constitute specific legal advice.

Criminal offences

Intimidation, harassment and threatening behaviours

Threatening behaviour

This includes threatening to, kill or do grievous bodily harm, destroy property or to cause harm to people or property. Examples are, comments on social media sites that include a threat to life or destruction of property. If threatening behaviour is implicated in an incident, it should be reported to the police.

Relevant legislation: Crimes Act 1961, Section 306 & 307

Intimidating behaviour

This involves actions that intend to frighten or intimidate another person.
Examples are private messages sent via a mobile application that include threats to injure a person or any member of his or her family, or to damage any of that person's property.

Relevant legislation: Summary Offences Act 1981, Section 21

Harassing behaviour

This involves harassing another person with the intent of causing them to fear for their safety or the safety of their family. An example is creating a social media account under a pseudonym that is used to post personal information about another person such as posting photos of where they live.

Relevant legislation: Harassment Act 1997, Section 8 / Telecommunications Act 2001, Section 112

Aiding and abetting suicide

This involves inciting or counselling someone to commit or attempt to commit suicide. An example is an internet 'troll' repeatedly goading someone to kill him or herself.

Relevant legislation: Crimes Act 1961, Section 179

Intimate photos or videos

This relates to making or posting online, sexually explicit photos or videos of a person that were made without that person's knowledge or consent.

Relevant legislation: Crimes Act 1961, Section 216H, 216I, 216J.

Online Grooming

This relates to an adult using the internet to manipulate and gain trust of a minor as a first step towards the future sexual abuse, production of objectionable material, or exposure of that to a minor.

Relevant legislation: Crimes Act 1961, Section 131B & 98AA.

Unauthorised access to an online account

This relates to anyone gaining access to a social media account without the authorisation of its owner. For example, taking over a school's social media account, changing the passwords to prevent access and then using it to harass members of staff.

Relevant legislation: Crimes Act 1961, Section 249 & 252

Objectionable and restricted material

Objectionable material

Any digital content or communication is objectionable if it "describes, depicts or expresses, or otherwise deals with matters such as sex, horror, crime, cruelty or violence in such a manner that the availability of the publication is likely to be injurious to the public good."12 All objectionable material is banned. A person could have committed an offence if, for example, they collect or view online images of sexual conduct involving children.

The Department of Internal Affairs (DIA) investigates and sometimes prosecutes people who deliberately collect objectionable material and find ways to distribute it to other people via the internet. Occasionally, the nature of the internet can lead to somebody viewing objectionable material by accident. This is one reason why searching a device or requesting digital content to be forwarded to a teacher or authorised staff member is not advisable.

Objectionable material can be reported through either:

DIA Content Complaint Form(external link)
The Online Reporting Button (ORB)(external link)

The DIA has implemented an internet and website filtering system known as the Digital Child Exploitation Filtering System (DCEFS) to block websites that host child sexual abuse images. This is available to all New Zealand Internet Service Providers (ISPs) on a voluntary basis. The Network for Learning's (N4L) managed network uses the DCEFS on the internet services it provides to schools.

If your school is with a different provider, you can check to see if its services apply the DCEFS(external link).

The DCEFS significantly reduces, but does not eliminate, the chances of accidental access to objectionable material online. More information on the DCEFS system(external link)

Relevant legislation: Films, Videos, and Publications Classification Act 1993, Section 123 & 131

Restricted material

Restricted material is made available to people who are over a certain age using a rating system, such as that used in New Zealand for movies; G, PG, M, R16 and R18. A person could have committed an offence if, for example, they were an adult sending sexually explicit text or images to a person under 18.

Relevant legislation: Films, Videos, and Publications Classification Act 1993, Crimes Act 1961.

Blackmail

This involves threatening, expressly or by implication, to make any accusation against any person to disclose something about any person or to cause serious damage to property or endanger the safety of any person with intent. An example would be a person threatening to publish an intimate recording unless more recordings or money were forthcoming.

Relevant legislation: Crimes Act 1961, Section 237

Scam or Fraud

This relates to using the internet to either obtain money or to cause loss by deception. An example is accessing a computer system for dishonest purposes, or conspiring to bring false accusation, or forgery.

Relevant legislation: Crimes Act 1961, Section 115, 228, 240, 249 & 256

Civil law

Civil law covers disputes between individuals, companies and sometimes local or central government. Civil law disputes are generally the cases in court that are not about breaking a criminal law.

New Zealand's civil justice system works in such a way that cases can be resolved through a claims process. Both parties are encouraged to find a resolution which means it is not always necessary to go to court.

Defamation

This means damaging the good reputation of someone by making slanderous or libellous statements.

Relevant legislation: Defamation Act 1992.

Discrimination

Discrimination occurs where a distinction is drawn between people on the basis of a personal characteristic, and that distinction leads to actual or assumed disadvantage.

Relevant legislation: Human Rights Act 1993, Section 21.

Harassment

Directing specified acts such as giving offensive material to someone or entering or interfering with their property.

Relevant legislation: Harassment Act 1997, Section 3 & 4, Part 3.

Breach of Privacy

The Privacy Act 2020 controls how personal information is collected, used, disclosed, stored and accessed.

Relevant legislation: Privacy Act 2020, Part 5.

References

A qualitative study of children, young people and 'sexting': A report prepared for the NSPCC. J. Ringrose et al (2012)

About civil law, Ministry of Justice, New Zealand [retrieved December 2014]

Advice on copyright in schools, Te Kete Ipurangi, Ministry of Education [retrieved September 2014]

Bullying prevention and response: A guide for schools. Ministry of Education (2014)

Children and the Internet: Great Expectations, Challenging Realities. Livingstone, S. (2009)

Children's Online Privacy Protection Rule (COPPA), Federal Trade Commission, USA(external link) [retrieved September 2014]

Children, risk and safety on the internet. Research and policy perspectives in comparative perspective. Edited by S. Livingstone, L. Haddon & A. Görzig (2012)

Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. Hasebrink, U., Livingstone, S., & Haddon, L. (2008)

Digital Citizenship in New Zealand School; Overview, NetSafe (2010)

Education Amendment Act 2013, New Zealand Legislation (2014)(external link)

Education Law Intensive 2012 (p10-12). Chair: Walsh, P. Continuing Legal Education, New Zealand Law Society (2012)

Enhancing child safety and online technologies: Final report of the Internet Safety Technical Task Force to the multi-state working group on social networking of State Attorneys General of the United States. Internet Safety Technical Task Force [ISTFF]. (2008)

Examining characteristics and associated distress related to Internet harassment: Findings from the Second Youth Internet Safety Survey. Ybarra, M. L., Mitchell, K. J., Wolak, J., and Finkelhor, D. (2006)

Good Practice Guide for Digital Evidence. UK Association of Chief Police Officers. (Version 5, 2011)

Guidelines for the surrender and retention of property and searches, Ministry of Education (2014)

Handling Mobile Devices – Blocking Network Connection. Advice to Police Officers. Electronic Crime Laboratory, New Zealand Police [Advice received September 2014]

Household Use of Information and Communication Technology: 2012, Statistics New Zealand (2013)

Information & Communications Technology in New Zealand Schools, 2020 Trust, New Zealand (2011)

Information Privacy Principles, Privacy Commissioner, New Zealand(external link) [retrieved September 2014]

New Zealand eGeneration study 2005: Kids and Teens Online. Reddington, J. (2005)

New Zealand Legislation, Ministry of Justice, New Zealand(external link) [retrieved September 2014]

Privacy in Schools: A guide to the Privacy Act for principals, teachers and boards of trustees, Privacy Commissioner (2009)

Protecting and promoting: An integrative conceptual model for healthy development of adolescents. Kia-Keating, M., Dowdy, E., Morgan, M. L., & Noam, G. G. (2011)

Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. Sourander, A. et al (2010)

Safer Children in a Digital World: A Report of the Byron Review. Byron, T. (2008)

The 'digital challenges' model. Cocker, M. NetSafe, New Zealand (2013) [retrieved December 2014]

The Informed Consent Process and the Application of the Code to Children, Annie Fraser, Office of the Health & Disability Commissioner, New Zealand (1998)

The Online Generation Gap - Contrasting attitudes and behaviors of parents and teens. Family Online Safety Institute, USA (2012)

To tell or not to tell? Youth's responses to unwanted Internet experiences. Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013)

Trends in youth internet victimization: Findings from three youth internet safety surveys 2000–2010. Jones, L. M., Mitchell, K. J., & Finkelhor, D. (2012).