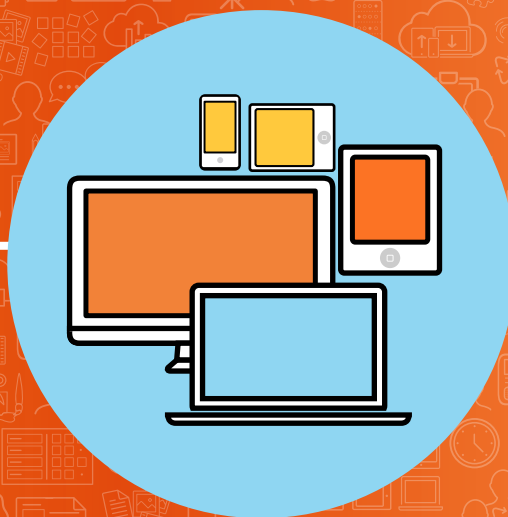




# A Quick Guide to technology compliance & legislation in schools





# Contents

01	<b>Introduction</b>
02	<b>Data protection advice for schools</b>
09	<b>Keeping pupils safe online</b>
13	<b>Copyright compliance in education</b>
15	<b>Digital literacy and online safety legislation</b>
18	<b>Health and Safety regulations in schools</b>

A young boy with blonde hair and black-rimmed glasses is looking intently at a white tablet computer. He is sitting at a desk in a classroom. In the background, a girl with dark hair is also looking down. On the wall behind them are several educational posters, including one of a tree and another with a red heart. The lighting is bright and even.

# Keeping your students and school safe online

In 2016, the latest version of the 'keeping children safe in education' guidance came into force. This applies to all children under 18, unless they are in a 16-19 academy/free school. However, when it comes to online safety, the advice remains limited.

As such, many schools have struggled to keep up with changes in the rules covering the use of technology, and this could leave students - and educators - vulnerable.

In this short guide, we set out some of the critical legislation that impacts the use of tech in schools, and what you need to do to ensure compliance, and keep your pupils safe.

The information contained in this guide is for general guidance only. As such, it should not be used as a substitute for proper legal advice. Schools should always seek professional guidance to ensure compliance with the law.

# Data protection advice for schools

The Data Protection Act (DPA) exists to protect the privacy of individuals. In an educational context, this means students, families, and staff.

**Here are some of the steps your school needs to take to ensure compliance with the Act:**

- ▶ **Register with the Information Commissioner's Office (ICO).** Each school must notify the ICO about how they process personal information. Registration can be done online, and failure to do so is a criminal offence
- ▶ **Comply with fair processing/privacy notices.** You must set out the data you require, why you need it, and which third parties it may be passed on to (e.g. other schools, social services, etc.). Primary and secondary schools have different data requirements, so will require different notices. You must also obtain consent from those people the information is about. Find out more



- ▶ **Respond to information access requests.** Students have the right to see their personal information should they ask for it. Parents DON'T have the right to access their child's personal data unless the child has provided consent (or is unable to act on their own behalf). Schools must, therefore, consider whether a pupil is old enough to understand their rights before responding to any request. Parents DO have the right to see their child's educational records. [Find out more](#)
  
- ▶ **Keep information secure and prevent breaches.** All personal information must be kept safe with security measures that are appropriate to the data held. This could include things like:
  - Using strong passwords
  - Shredding confidential waste and making sure electronic data is correctly destroyed
  - Encrypting electronic data
  - Installing firewalls and antivirus software
  - Keeping devices locked away when not in use
  - Disabling 'auto-complete' settings
  - Checking any data suppliers comply with the necessary regulations.

Where you fail in your duty to put adequate security measure in place, the ICO can issue fines



- **Put additional processes in place for Sensitive Personal Identifiable Information (SPII).** SPII comes with greater legal restrictions. SPII includes information such as name, date of birth, address, etc., and things such as race or ethnicity, religious beliefs, physical or mental health, sexuality, and criminal offences. Make sure any SPII your school holds is processed and stored with extra care
- **Ensure adequate training.** As well as having an understanding of the DPA, school employees should receive extra training to help keep pupils safe. The ICO has a wealth of information to help SMTs put adequate data protection policies and training in place.  
[Find out more](#)



- **Hold regular information audits.** If you keep data for longer than it is needed, you will violate the DPA. You must also make sure any data held is up-to-date. To help you to do this, carry out an information audit at least once a year. This includes asking parents to check their details are correct (make sure you stay compliant while doing so!), making any changes to your systems, and destroying data you no longer need.

[Find more help on this here](#)

- **Establish data protection roles.** Get help by appointing specific individuals to help you implement and uphold data protection in your school. For example:

- Senior Information Risk Officer to oversee risk-reduction strategies and processes
- Information Asset Owner responsible for compiling and/or working with specific personal information.

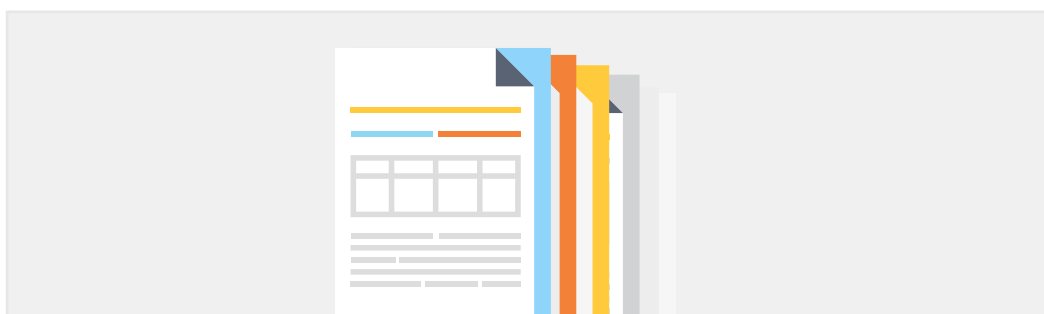
[Find out more](#)

- Data Processors who act on behalf of the school to help implement security measures and protect personal data. However, the school - as the Data Controller - retains overall responsibility under the Data Protection Act.

Anyone who takes on a specific data protection role should receive adequate training to help them with this.



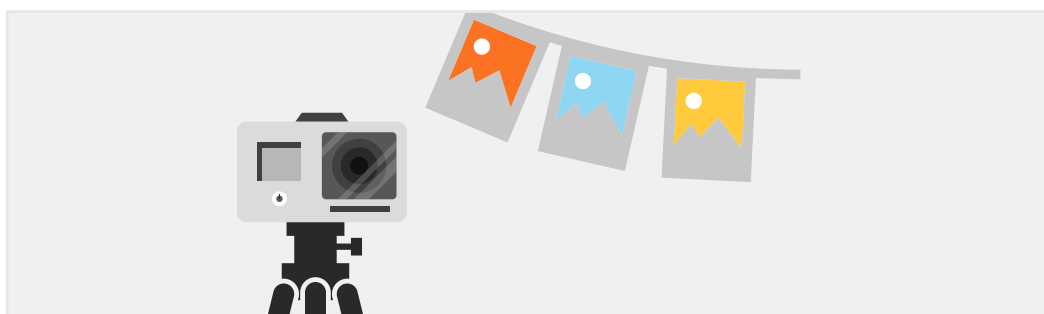
## Here are some examples of how schools must comply with the DPA:



### Publishing exam results

The DPA does not stop the publishing of examination results by schools, (e.g. in the local press). But, schools have to act fairly when publishing results and must take seriously any concerns raised. For example, some pupils might object if results are to be published in grade order.

[Find out more.](#)



### Using photography and videos

Photos and videos taken for official school use may be covered by the DPA and students and parents should be advised why they are being taken and where they will be used. [Find out more.](#)



# To help ensure compliance in your school, create an Acceptable Use Policy (AUP).

An AUP will ensure everyone knows what is and isn't acceptable when it comes to using tech in schools. This should cover things such as:



Parental permission



A website privacy statement which states how information is acquired and how it will be used



Email and how personal data is shared between students and staff. (e.g. when sending bulk emails, making sure staff don't use the BCC function, so that parent and pupils emails are not disclosed)



School websites. With policies on using student images and names




Guidance on logging off or locking devices when not in use



Guidance on physically storing mobile devices to minimise loss by theft



Making sure all IT equipment is asset tagged with identifiable serial numbers and locations so that in the event of theft, items can be accounted for.



Your policy should also take into account the latest guidance from the UK Council for Child Internet Safety (UKCCIS). [Access the latest and full UKCCIS guidance here.](#)

---

Make sure your sure teachers understand the AUP to protect your school and its data. Students should also be taught never to give out personal data as part of e-safety education. [Find out more on the latest government guidance on how schools should protect data online.](#)

---

**From May next year**, schools will also have to comply with the new General Data Protection Regulations. SMTs must act now to ensure they are aware of the potential steps, costs, and resources required.

# Keeping pupils safe online



**In 2015, security issues occupied the bottom slots of the top ten areas of concern for CIOs and IT leaders in education. In 2016 and 2017, Information Security was considered the number one IT issue.<sup>1</sup>**

The Act can also be unwittingly breached. For example, a student who knowingly goes into another student's Facebook account without their permission is breaking the law. However, many schools are unsure what to do when they uncover unauthorised access to their IT systems.

<sup>1</sup>[Citation](#)



The Computer Misuse Act discourages people from using computers for illegal purposes. There are three parts to the Act:



Unauthorised access (hacking)



Accessing material with the intention to commit illegal activity (e.g. fraud, blackmail, etc.)



Making changes to data stored on a computer without permission (e.g. installing malware or viruses).



## The following tips will help you comply with any legal issue with technology in education:

### Awareness

- Undertake a thorough and ongoing risk assessment.

### Education

- Make sure students are aware of the illegality of hacking. In many cases, they don't realise that a simple "prank", could lead to them getting in trouble with the police
- Train teachers, pupils and other staff on how to respond to any suspicious emails or other breaches.

### Improve your technology

- Every device and application you use has the potential to be a point of weakness in your school's network
- Consider using educational technology that has been designed specifically for schools
- Regular software updates are also important to help keep your IT secure.

### Reporting

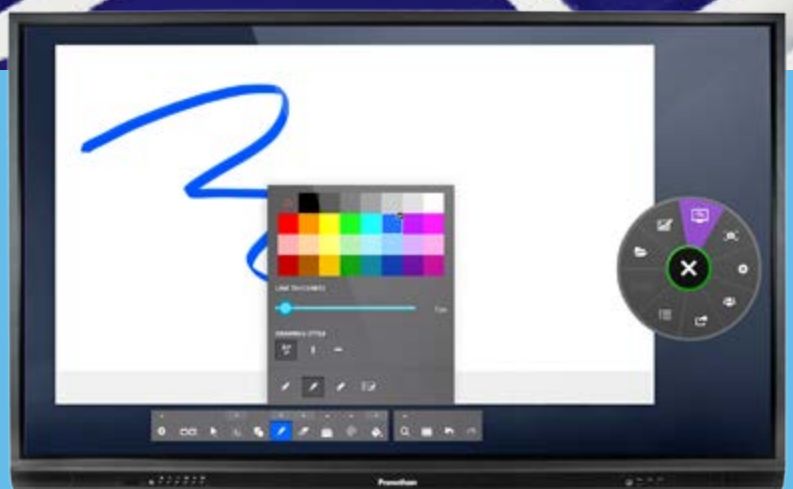
- Put processes in place that deal with the reporting and tracking of security incidents
- Make sure any and all breaches are reported to the Police, Action Fraud, and the ICO.

## Security processes

- Ensure your school has appropriate filters and monitoring systems in place. According to government guidance, "the appropriateness of any filters and monitoring systems are a matter for individual schools".  
The UK Safer Internet Centre has published guidance as to what "appropriate" might look like
- Review your policy on the use of mobile technology. This should cover things such as how to deal with students bypassing the school network and accessing the internet through 3G and 4G connections
- Deploy an appropriate anti-virus system
- Ensure ALL software and OSs are up to date and have the latest security updates installed
- Make sure your system updates automatically (ideally daily)
- Make sure that backup procedures are in place and that they are up to the job
- Make sure strong passwords are in place as standard.

## TIP:

ActivPanels from Promethean are ideal for use in a school environment and help to provide a safe 21st Century Learning environment.



# Copyright compliance in education

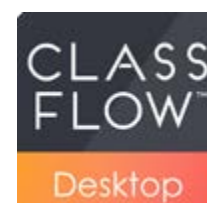
The Copyright, Designs and Patents Act gives the creators of literary, dramatic, musical, and artistic work the right to control how their material is used. Schools need to be aware of how this legislation affects the use of material taken from the internet.

Copyrighted materials can be used without permission in some educational circumstances due to 'fair use' policy. This establishes the right to use portions of copyrighted materials, without authorisation, for purposes of education, commentary, or parody. However, while a lot of material is okay for use under the educational umbrella, when added to websites or lesson plans, schools could be facilitating the free redistribution of such material, and this could lead to problems.



## The following tips will help you comply with the Copyright, Design and Patents Act:

- ▶ Create a copyright policy and make sure all teachers are aware of it
- ▶ Instead of giving out printed handouts, teachers can provide pupils with a link to the information they need. Combining an ActivPanel and student laptop/mobile devices is an excellent way to do this
- ▶ Use Creative Commons (CC) work rather than those with “all rights reserved”. There is a plethora of these freely available on sites such as Flickr and YouTube
- ▶ Most web services and content sharing networks (e.g. YouTube, Wikis, etc.), don’t require a copyright licence. However, each platform has its own T&Cs so make sure you are aware of these
- ▶ Use sites that offer free educational resources that can be incorporated into lessons. For example, ClassFlow provides a wealth of ready-made activities and content
- ▶ Create and deliver lessons on the importance of copyright. This will help pupils as they move to the workplace where such issues are of particular relevance.





# Digital literacy and online safety legislation



**Two-thirds of teachers are aware of pupils sharing inappropriate sexual content, with as many as one in six of these children of primary school age.**

NASUWT teaching union

While it has the potential to deliver immense value, our online world also comes with inherent risks; particularly for children. Digital platforms make children vulnerable to criminals and bullies. And, in the worst cases, leave pupils open to manipulation and abuse. In fact, while younger generations are being labelled as “digital natives” when it comes to safety, they are often no more literate than their parents.

To mitigate harm, England, Scotland, Northern Ireland, and Wales all have specific guidance setting out how educators must protect children from harm online. These guidelines - which are based on various pieces of legislation - cover online grooming, sexual exploitation, cyberbullying, and sexting.

A background image showing several children in a classroom setting. In the foreground, a child's hand is visible interacting with a tablet. To the left, another child is looking down at a device. In the upper right, a boy is seen from the side, resting his head on his hand. The overall scene is a typical classroom environment with children engaged with technology.

**The following tips will help you comply with the various legislation, and keep pupils safe online:**

- ▶ Teach students about online risks, how to recognise unsafe online contact, and what material is/is not appropriate to share
- ▶ Ensure students know how to report anything that makes them uncomfortable and any concerns they may have for themselves or another pupil
- ▶ Put robust processes in place to respond to any incidents
- ▶ Identify a lead member of staff for to provide governance and act as a single point of contact when it comes to reporting or finding out more information about child sexual exploitation.

**Ensure your e-safety procedures are robust. Here are some resources to help you to do this:**

- ▶ Access [guidance](#), to help you embed cyberbullying in your anti-bullying work
- ▶ Read the [latest guidance for Ofsted inspectors](#) when inspecting safeguarding under the common inspection framework
- ▶ Access statutory guidance on [Keeping Children Safe in Education](#)
- ▶ Read [Sexting in schools and colleges](#): Responding to incidents and safeguarding young people
- ▶ Visit [360 degree safe](#), a free, self-review online tool for schools
- ▶ The [NSPCC has also collated lesson plans and online guidance](#) to help teachers boost digital literacy in their classrooms
- ▶ [eCadets](#) is the UK's leading pupil-led online safety education programme.



# Health & Safety regulations in schools

Every school has a health and safety policy, and a responsibility to make sure ICT equipment is used correctly and safely.

## The following tips will help you comply with health and safety legislation:

- ▶ Make sure all IT equipment is PAT Tested and safe to use
- ▶ Advise pupils and teachers about good practice when using computers
- ▶ Put cable management systems in place to mitigate trips and falls
- ▶ Take any damaged equipment out of service to be repaired or replaced.



# In conclusion

Despite the latest DfE guidance detailing the legal duties schools must comply with to keep children safe, some schools are failing in their safeguarding obligations. Often because this information is not as comprehensive as it should be. So it is up to schools to make sure they are aware of their wider legal requirements.

In addition, to help headteachers ensure compliance, they should look to invest in technology that has been designed specifically for use in an educational context; with all the safety measures this ensures.

Find out more about ActivPanel and how it can help schools create a safe and dynamic educational experience.

**Find out more** ➔



