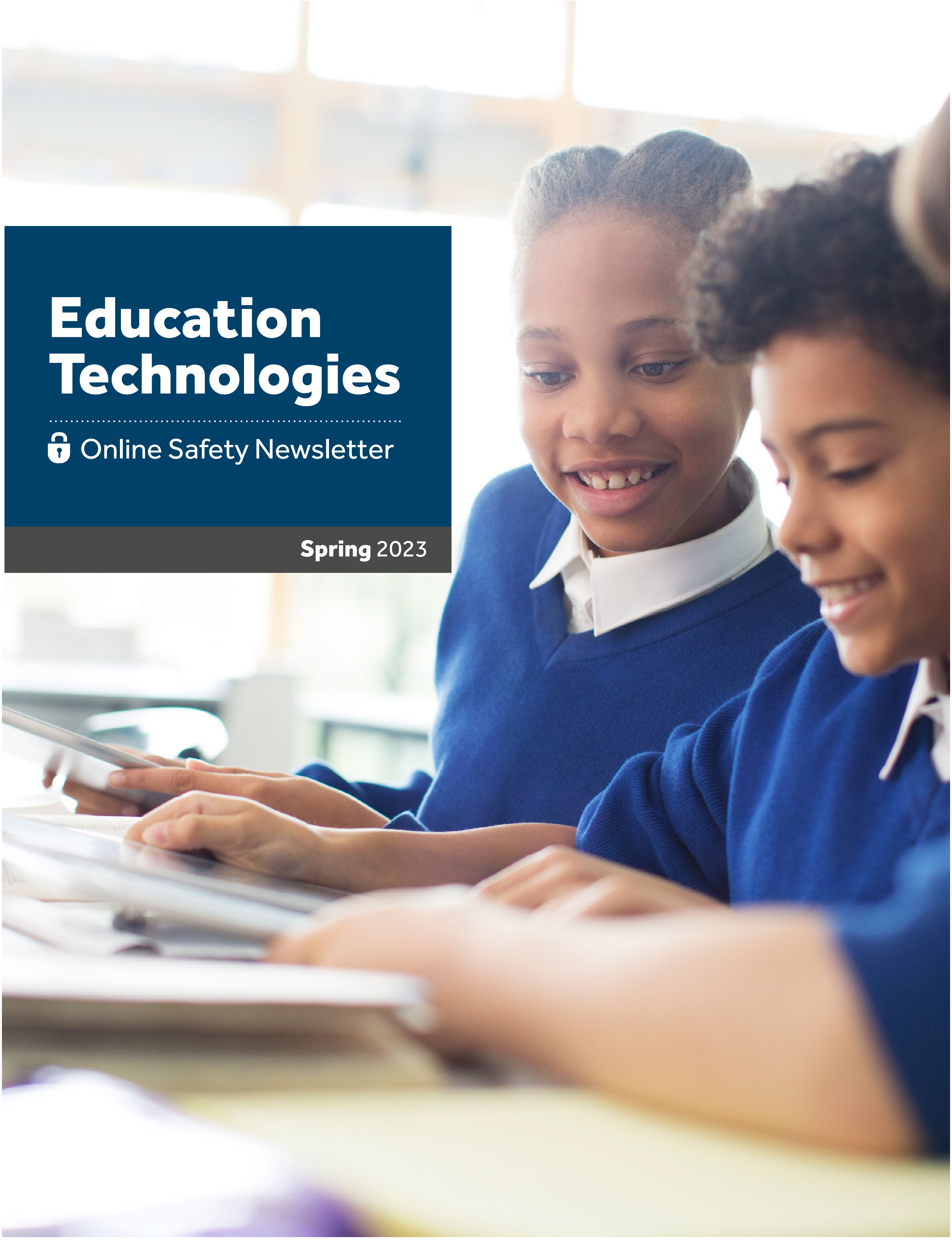


Education Technologies

Online Safety Newsletter

Spring 2023

Call **0333 300 1900** Email **information@entrust-ed.co.uk**
or visit **www.entrust-ed.co.uk** to find out more about our services.

Entrust Education Improvement Entrust Support Services Limited @entrustEDU

entrust
Inspiring Futures

Welcome

We trust you are all keeping safe and well. Please feel free to share this newsletter with other members of staff from your school. If they wish to subscribe visit Subscribe to Entrust's online safety newsletter.

We hope you find the newsletter useful and if you have any feedback about our service to schools or anything you would like to see in next term's update, please do not hesitate to let us know by emailing **information@entrust-ed.co.uk**

Harmful sexual behaviour guidance and resources

The centre of expertise on child sexual abuse have produced a **series of free guides**, specifically for those working in education settings, to help guide effective responses when they have a concern of child sexual abuse or behaviour.

Intentional use – how agency supports young people's wellbeing in a digital world

Internet Matters has produced **a report** that explores how the mindful use of digital technology can benefit our wellbeing. Using the example of managing screen time, it shows the value of not just counting time spent online but also reflecting on what we are doing with that time and how that makes us feel.

Grandparents guide to online safety

How many grandparents help out with childcare and may benefit from getting to grips with life online? Internet Matters have produced a grandparents guide to online safety.

Foster carers – Enable

Enable – making a difference to the digital lives of young people. Enable offers unique support, training and tools to foster carers to help children flourish online. It is created by online safety specialists and psychologists, with foster carers and young people. The resource library is packed with a wealth of resources that are topic based around a young persons life online.

Mental health of children and young people

NHS Digital has published the wave 3 follow up survey to the 2017 survey.

Some of the key findings include:

- 1 in 8 (12.6%) 11 to 16 year old social media users reported that they had been bullied online. This was more than 1 in 4 (29.4%) among those with a probable mental disorder.
- 11 to 16 year old social media users with a probable mental disorder were less likely to report feeling safe online (48.4%) than those unlikely to have a disorder (66.5%).

Digital matters

The easy way to teach your students about online safety

Digital Matters is a free, interactive learning platform that teaches KS2 students about online safety. Created by Internet Matters, and with links to the curriculum, it includes modules on topics like Online Relationships, Privacy & Security, and Online Bullying.

It offers lesson plans, resources, and interactive activities to engage students and support teaching, as well as resources for parents to encourage further learning at home.

Internet Matters is also offering a chance for teachers to win up to £300 for their school by signing up for Digital Matters and answering a simple question.

CLICK HERE TO ENTER

Harmful sexual behaviour support service has now closed!

In March 2022 the support service began as a pilot project funded by the Home Office and in collaboration with the DfE. The pilot has now come to end and the support service has closed.

In response to this closure, ourselves and the Marie Collins Foundation are providing guidance and resources, and an online video training package, which will continue to provide support to professionals. If you have any queries please contact media@swgfl.org.uk

Teaching online safety in schools – guidance updated

Updated 12th January 2023. Non-statutory guidance outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.
It complements existing subjects including:

- relationships education
- relationships and sex education
- health education
- citizenship
- computing

Migrating to securus software as our recommended digital monitoring software

Staff at Entrust have been evaluating and recommending appropriate monitoring software to schools for over 15 years and we have recently made the decision to move over to Securus Software as our recommended product.

There are a range of different monitoring software providers, and all of these will monitor for keywords that the pupil types on the keyboard. However, Securus is the only one of the main providers that will also scan for inappropriate words or phrases that are displayed on the screen.

Why is this important?

The 4Cs classification recognises that online risks arise when a child:

- engages with and/or is exposed to potentially harmful CONTENT;
- experiences and/or is targeted by potentially harmful CONTACT;
- witnesses, participates in and/or is a victim of potentially harmful CONDUCT;
- is party to and/or exploited by a potentially harmful CONTRACT.

In the highlighted portions of the points above, the risks are all posed by a third party and are not through the actions of the child, that is, they have not typed something on the keyboard that will be picked up by the other monitoring software. It is the information that is displayed on the screen that is key to identifying the issue. To put this into context, on the Entrust Digital Monitoring Service 80% of the escalated captures sent to school are generated from desktop content and not what the pupil has typed on the screen.

In practice this means, amongst other things:

- A pupil mis-spelling a search that returns inappropriate results or clicking a web link that sends them to an inappropriate site.
- Receiving an email that says 'kill yourself'
- Receiving sexual or coercive DM's
- Receiving threatening, bullying, radicalising or grooming messages over chat or email
- Reading and clicking links in SPAM emails
- Joining inappropriate Discord servers or reading age-inappropriate fan fiction

In each of these cases, the pupil has not typed anything that would trigger other monitoring software and the issues would be missed but, because Securus is scanning the keyboard AND screen you will receive captures that highlight the risk.

If your school is currently reviewing the monitoring software used, please ensure that the safeguarding leads are included in any evaluation and you understand exactly what is being monitored and captured - the above bullet points could form questions to ask prospective suppliers how their software would react. We are always happy to discuss what constitutes appropriate filtering and monitoring for schools and if you would like any more information please get in touch.

FREE

Online Safety Conference 2023

Making Space for Conversations about Life Online

1st February 2023, 8.30am – 4pm
Virtual Delivery

BOOK YOUR PLACE NOW!

Keynote speakers include:

- **Graham Lowe** from Safer Internet introducing developments in the online landscape and its impact for safeguarding our children & young people as well as highlighting important supporting tools and resources that will help guide practitioners to develop online safety provision in their setting.
- **Carmel Glassbrook** from the Professionals Online Safety Helpline (UK Safer Internet) who will be identifying trends, and issues from the Professionals Online Safety Helpline and learning from the Harmful Sexual Behaviour Support Service.
- **Simone Vibert** from Internet Matters will be discussing Changing Conversations and sharing some brilliant resources from The Digital Inclusion Hub.
- **Cormac Nolan** from NSPCC Childline will provide stories from Childline and how teachers can make use of Childline resources.
- **Sally Sparrow** from The Safeguarding Company will explore what the data behind My Concern is telling us about to the lives of young people today.
- **Alan Merrett** from the National Crime Agency will explain how the average age of a hacker for those referred to the National Crime Agency for cyber-crimes is reducing, and what this means for schools in both secondary and primary settings.

CLICK HERE TO BOOK

Radicalisation and Extremism

What impact have lockdowns and their aftermath had on the spread of extremism?

BBC reported that online hate speech had increased by 20% during the pandemic

The United Nations produced a report last year looking at how the pandemic has fueled terrorism and violent extremism. The messaging app and social network Telegram rapidly grew during the pandemic and became a hub for 'disinformation through to conspiracy theories, through to terrorist activity' due to its very unmoderated approach.

A school's safeguarding responsibilities, should help students build resilience against extremism and radicalisation by fostering a strong ethos and values-based education, as well as by providing a safe space for them to debate controversial issues and develop the critical thinking skills and knowledge they need to be able to challenge extremist arguments. There are some excellent resources for school leaders, teachers and parents regarding radicalisation and extremism at educate against hate.

The Prevent Duty places emphasis on the need to prevent pupils from falling under the influence of extremist ideas and integrate this into the school's ongoing safeguarding role and syllabus. The 2011 Prevent strategy has three specific strategic objectives:

- respond to the ideological challenge of terrorism and the threat we face from those who promote it
- prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support
- work with sectors and institutions where there are risks of radicalisation that we need to address.

How informed are our students of what hate speech is and are given space to debate controversial issues within the curriculum? Are they and their parents/ carers informed enough to recognise it online and know how they can keep safe online from the risk of radicalisation?

What about influences from the likes of self-proclaimed 'misogynist', controversial influencer Andrew Tate recently arrested on suspicion of human trafficking. His views being described as extreme misogyny, capable of radicalizing men and boys to commit harm offline appears to be held hero to many young men and boys with schools and parents expressing concerns.

The Keeping Children Safe in Education 2022 statutory guidance part 5 is about how schools and colleges should respond to all signs, reports and concerns of child-on-child sexual violence and sexual harassment, including those that have happened outside of the school or college premises, and/or online.

Following Ofsted's review into sexual abuse in schools and colleges reported that the frequency of harmful sexual behaviours was sufficiently widespread that the review reported that children viewed them as normal.

Ofsted advised that:

> *"Should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports" They made it clear that there is a "zero-tolerance approach to sexual violence and sexual harassment, that it is never acceptable, and it will not be tolerated."*

How are schools and colleges challenging attitudes? What is your approach to education, policy and procedure? Is there a transparency of process and consequences? An interesting reflection on education with suggestions for schools can be **found here.**

Safer Internet Day 2023

7th February 2023 is Safer Internet Day and the theme is 'Want to talk about it? Making space for conversations about life online'.

You can register your school's support and resources will be made available.

Cyber and Data Security

School hit by cyber-attack and documents leaked

Pates Grammar School in Gloucestershire was targeted by hackers. Highly confidential documents including children's SEN information, child passport scans, staff pay scales and contract details from 14 schools were leaked online when the ransom payment was not made.

The initial attack is estimated to have taken place on 28 September 2022, the hackers would have sat quietly on the network carrying out reconnaissance work, finding the data they require, taking copies and then unleashing the ransomware. The school is working with highly experienced forensic investigators to secure their systems and resolve the issue. Full details on this incident can be found **here**. Confidentiality, integrity and availability of personal data has been affected and the ramifications for the school could be extremely damaging to reputation and finances. The school can't operate without access to their systems and data which is being held to ransom and therefore must close. Systems need support from professional agencies to scan devices, remove the ransomware and rebuild work stations – this takes time and money. Not to mention the considerable distress to the individuals involved.

Schools and colleges need to be confident in the cyber security measures they have in place to know that in the event of a cyber incident they can restore and recover from the incident with minimal disruption and damage. The threat of a cyber attack can never be removed, organisations have to be ready when it does happen. How prepared is your organisation? Have you discussed your risk appetite and attitude towards a threat? What organisational and technical measures have been put in place, led by strategic decision making, to protect your critical assets? What is and isn't covered by the technical measures and support you already have?

Do you know who a cyber incident should be reported to?

Knowing who to report to in the event of a cyber-attack is part of your legal obligations and is a requirement of standard 10 of the DfE guidance **cyber security standards** for schools and colleges that was shared with you in the previous newsletter.

The data breach faced by Pate Grammar School poses a risk to an individual's rights and freedoms and therefore must be reported to the Information Commissioners Office within 72 hours after having become aware of the breach. In addition to notifying the ICO, the data breach also poses a high risk to those individual's affected so all individual's involved should also be informed. Schools and colleges must also report cyber attacks to **Action Fraud** and DfE sector cyber team at Sector.Incidentreporting@education.gov.uk and must act in accordance with the ESFA Academy Trust Handbook Part 6.

For phishing emails, you are not required to report to the DfE or Action Fraud. Instead, you can report to report@phishing.gov.uk

Get help with cyber security

Entrust can help with keeping your school safe and secure. To find out more please call **0333 300 1900** or email **information@entrust-ed.co.uk**

National Cyber Security Centre Training

One of the conditions for cover under the DfE RPA arrangement for cyber insurance is that all employees or governors who have access to the member's information technology system must undertake NCSC training. In the event of a claim the member will be required to evidence that any employee or governor involved in the claim has undertaken the NCSC training. NCSC training is available free of charge for schools to access.

A school may instruct all staff to complete the 30 minute module independently, however this does not allow for staff to ask any questions or to seek further clarification on something. The material is also available for a member of staff in school to lead a session with all staff, however if the staff member leading is not very confident with cyber security then this can be daunting and challenging.

We can provide a knowledgeable consultant to deliver the NCSC training materials to your school staff with the opportunity to ask further questions regarding cyber security. This ensures that all staff who are present at the session have received all the relevant information from the training materials, are aware of cyber risks and meets one of the conditions for the RPA cover. This session will be delivered remotely to schools, options for face to face training is negotiable dependant on location.

FIND OUT MORE

Should you require support in delivering this training resource, please contact information@entrust-ed.co.uk for more details

Cyber Sessions for Schools and Colleges

Entrust have been supporting leaders of schools and colleges to become aware of some of the issues the education sector is facing from the cyber threat landscape and why it is so important that there is a cyber response plan in place that covers strategic and technical decisions.

These hour-long webinars are free to attend, one is aimed at head teachers and senior leaders and the other is aimed at governors and trust members.

What do I need to consider about cyber security in an education setting? **FREE**

This **FREE** session is aimed at head teachers, senior leaders, governors and boards to consider their own knowledge and understanding of the impact a cyber attack or security breach could have on their establishment. Take back questions to find out and improve a school's understanding of its cyber security risks and risk management processes and procedures.

Date: 15th February 2023 **Time**: 13:00-14:00 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**
Date: 6th March 2023 **Time**: 15:45-16:45 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**

Governing Body Role in Cyber Security - **FREE**

Governing board members do not need to be technical experts, but they do need to know enough about cyber security to be able to engage in conversations with technical experts and senior leaders and know the right questions to ask to understand the organisation's cyber security approach; to provide challenge, and to help steer the strategic direction of cyber security within the organization.

Date: 27th February 2023 **Time**: 17:30-18:30 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**
Date: 1st March 2023 **Time**: 09:30-10:30 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**

Already attended our free cyber webinars and are now ready to take action but are unsure how?

For those that attended the free initial cyber security awareness sessions and now need next steps or further support we have a more detailed cyber event that is framed around the National Cyber Security Centre '10 Steps to Cyber Security' guidance that will unravel each of the 10 steps and provide examples and guidance on what these steps could include for an education setting. References will also be made to the DfE's Cyber Security Standards for schools and colleges.

SPECIAL OFFER

We recognise the importance of strategic and technical decision making when it comes to cyber resilience, so we are giving all education establishments the opportunity for a senior leader along with a member of their internal technical staff to attend our in-depth course 'Cyber Security – steps to take'; at a reduced cost. The first place on the course will be charged in full £149 and the second place will be charged at **50% less at £74.50**. This is to encourage educational establishments to make joint strategic and technical decisions for cyber security.

The event details are as follows. Please pass this information on to your leadership team:

Cyber Security – Steps to Take

Aimed at head teachers, senior leaders, governors and boards to think proactively about cyber security to resist cyber threats and online security issues. Be aware of strategic, operational and technical elements that are required to work together to create effective layers of security to defend against cyber threats.

Date: 13th February 2023 **Time**: 09:30-15:00 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**
Date: 25th April 2023 **Time**: 09:30-15:00 **Venue**: Remote delivery via Microsoft Teams	**CLICK HERE TO BOOK**

NCA Cyber Choices Challenge 2023

#CYBERCHOICES

Get involved: https://cybergamesuk.com/cyber-choices-challenge

The Cyber Choices Challenge has arrived! Help Astro through the levels of the challenge and see if you can make it up to the top of the leader board. Get involved in the challenge and have the chance to win EGX 2023 tickets or Amazon vouchers. Good Luck! Make the right #CyberChoices and put your skills to good use.

Will you able to help Astro through the levels and earn yourself a place at the top of the Cyber Choices Challenge leader board? If you are up to the task then take part in Challenge for the chance to win top prizes and improve your knowledge of the Computer Misuse Act 1990.

There's still time left to help Astro through the Cyber Choices Challenge and get your name at the top of the leader board! Test your knowledge of the Computer Misuse Act 1990 for the chance of winning EGX 2023 tickets or Amazon vouchers. Good Luck!

> *"The NCA Cyber Choices Challenge 2023 aims to raise awareness of NCA Cyber Choices and Prevent programmes, and champion accessibility to cyber security skills education for 11-18 year olds in the UK."*

Early registration is open from Monday 16 January 2023, and ends at midnight on Sunday 29 January 2023. Complete the registration process now to score bonus points and get a head start on the leader board!

entrust
Inspiring Futures

Remote Courses from Entrust Ed Tech for Online Safety in Education Settings

To book your place please call 0333 300 1900 (option 3) or email enquiries@entrust-ed.co.uk

Online Safeguarding for Designated Safeguard Leads - £149 (+VAT)

DSL's that attended our recent Online Safety for DSL's 2-part webinar found the event and its contents extremely valuable, in particular:

- becoming familiar with the terminology and techniques used online when young people may be at risk;
- what we mean by peer-on-peer abuse online;
- discussing and identifying what can make a young person more vulnerable online and how they might be supported;
- monitoring and filtering implications for school owned devices on site and off site.

The next 2 x 2.5-hour webinars are:
Webinar 1 – 22nd March 2023 - 09:30 – 12:00
Webinar 2 – 24th March 2023 - 09:30 - 12:00

Booking Code: LTTL-OM-0323-T001

CLICK **HERE** TO BOOK

Online Safety in the Primary Curriculum - £99 (+VAT)

Examine the statutory online safety elements from Keeping Children Safe in Education and consider the Relationships and Health Education requirements alongside the programmes of study for computing in a primary school.

26th April - 09:30 – 11:30

Booking code: LTTL-OM-0423-T002

CLICK **HERE** TO BOOK

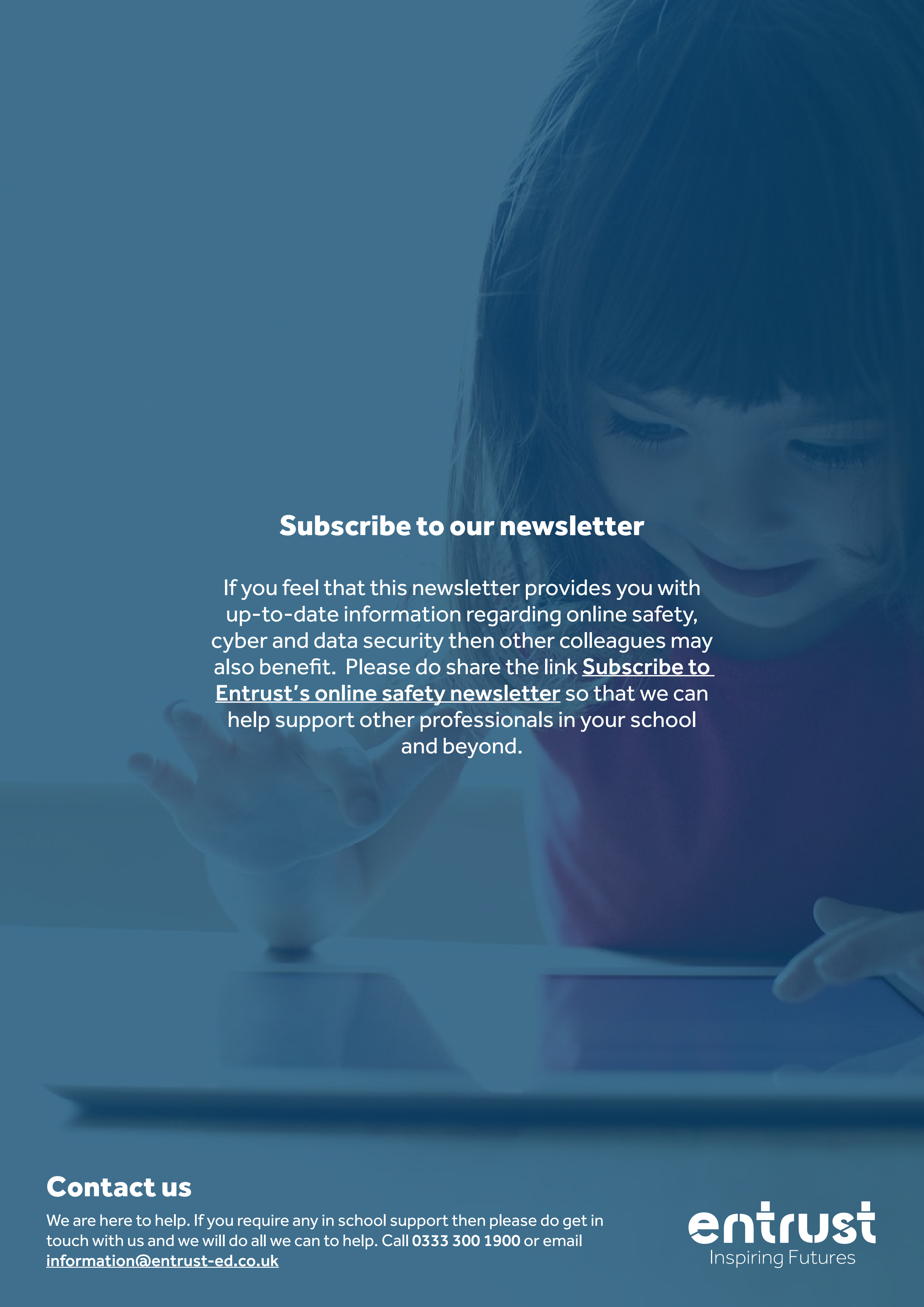
Leading Data Protection in Your School - £149 (+VAT)

Cyber security is part of your data protection duties to remain compliant with the Data Protection Act 2018. If you have any staff that are responsible for the day-to-day management of data protection within your school but would benefit from further understanding what is expected from this role and how they should work alongside the Data Protection Officer, then we do run a 2-part webinar:

Session 1 of 2: 13th March 2023 - 13:30 – 15:30
Session 2 of 2: 17th March 2023 - 13:30 – 15:30

Booking code:- LTTL-OM-0323-T002

CLICK **HERE** TO BOOK



Subscribe to our newsletter

If you feel that this newsletter provides you with up-to-date information regarding online safety, cyber and data security then other colleagues may also benefit. Please do share the link **Subscribe to Entrust's online safety newsletter** so that we can help support other professionals in your school and beyond.

Contact us

We are here to help. If you require any in school support then please do get in touch with us and we will do all we can to help. Call **0333 300 1900** or email **information@entrust-ed.co.uk**

entrust
Inspiring Futures