Inside this issue...

- GDPR
- Protex
- Talking to Parents about Online Safety
- essential e-safety
  E-Safety Conference

Autumn 2017
Online Safety Special
Conference 2017 The Digital School

This year’s conference may have been our last, or our last for a while, but we certainly finished on a high. Who could fail to be excited by Stephen Heppell’s vision for schools, inspired by Paul Curzon’s approach to teaching computational thinking or energised by Zoe Ross? And as for Evelyn Glennie - she was simply wonderful!

You, the delegates, have always been at the heart of the E2BN conference; without your enthusiasm and willingness to try new things and get involved it would have been a pointless exercise. It was lovely to see so many of you who have attended the conference for so many years and it was also exciting to welcome first time visitors.

It is remarkable to consider just how the E2BN conference has grown and developed over the years.

The first E2BN conference was a one day event back in 2001. There were maybe 60 people – mostly staff from the Local Authorities that had founded E2BN and I believe it was little dull! The following year the audience was bigger. John Davitt gave a keynote and he featured a digital video of a dog lip syncing to the two times tables. The audience was seriously impressed.

By 2000, the E2BN team had much bigger and grander ideas for the conference: two days, two dozen workshops, the best education technology presenters available and lots of exhibitors. From then on the E2BN team were on a mission to bring the very best, the very latest and the very coolest examples of education technology and the most relevant and up-to-date CPD to delegates.

Over the years, the conference saw the likes of: Alan November, Chris Yapp, Niel McLean, Russell Prue, Sir Bob Geldof, Maggie Philbin, Gareth Thomas and Simon Weston to delight, entertain, inform, inspire and sometimes bring tears to hundreds of delegates. And whilst these top flight, conference circuit professionals have wowed audiences, even more remarkable have been the dozens of ‘ordinary’ teachers and Headteachers who have also stood on that stage or in the workshop rooms and talked about the practical realities of technology in the classroom: people who have shared their successes, failures and ideas via the conference to benefit hundreds of unknown pupils in schools across the region.

For many delegates, the E2BN conference was about firsts: their first attempt at digital video editing, Video Conferencing, digital sound mixing, interactive whiteboards, coding, green screening, 3D printing, RFID (radio frequency identification), geocaching, school radio, Augmented Reality, virtual reality, drones, e-readers, blogging, web publishing (before it was social media), web quests, the Raspberry Pi. Or the first time they considered the risks that technologies could pose to young people or realised the extent to which it had permeated everyone’s lives. For some, it was the first time technology looked like it could be fun or, indeed, useful in the classroom.

Whilst the E2BN team are saddened by the decision not to hold the two day conference next year, they can look back over nearly 20 years of conference with a sense of pride. It has been a job well done!
E2BN Protex is a flexible and affordable filtering system that keeps your children safe by putting you in control of your pupils’ access to the Internet. Staff and pupils each have different filtering profiles. Subscribing to the Protex service enables your academy or school to tailor filtering to your own E-Safety policies.

**Key features and benefits**

- Safer Internet Centre Certified
- BYOD and Mobile Device Filtering
- Real-time Updates
- Dynamic Filtering
- UK Based Support
- Inappropriate Search Filtering
- Authenticated Access
- Comprehensive Reporting
- Flexible Filtering Profiles

**Coming Soon!**

Look out for our latest improvements:

- Protex Transparent HTTPS filtering
- Improved Administration Interface

We are planning to update the reporting facilities. If you have any suggestions as to what sort of information you would want from the reporting system please let Tom Smith know by email:

tom@e2bn.org

www.e2bn.org/cms/web-filtering/protext-web-filtering

---

**Courses at the E2BN Office**

**5th October** – *Computing is Fun!* Fantastic introduction to Computer Science for those who are new to teaching Computing or looking for more interesting ways to teach CS. How can ‘kidbots’, human databases, clapping games, flashing torches, whistles, broken PCs, running around in circles and generally having fun help children develop a deeper understanding of Computer Science? How did poor cyber security change the course of British history? How did Computer Science make it possible for a man with ‘locked-in syndrome’ to write a book? All will be revealed in this hands-on, interactive workshop. Free places for the first six delegates to book (one free place per school). More details and online booking:

www.e2bn.org/cms/events-and-training/new-to-computing-free-cpd

**18th October** – *Online Safety for Early Years.* Online safety for younger children is important but is often overlooked. This half day course will help delegates understand how to keep younger children safe online. Free places for the first six delegates to book (one free place per school/setting). More details and online booking:

www.e2bn.org/cms/online-safety-for-early-years

**Advance Notice**

**7th March 2018** – *Online Safety Leaders.* This one day course for online safety leaders, DSL and anyone with an online safety responsibility will reveal the latest apps and online technologies that young people are using, what Ofsted are looking for, which policies you actually need and how to manage sexting incidents in school. This course will be repeated on 18th April. This is a very popular course so please book early to secure your place. More details and online booking:

www.e2bn.org/cms/events-and-training/online-safety-leaders-day

**Courses at Your School**

The above sessions can be tailored to fit into a school INSET day or half day. A 90 minute version of Computing is Fun is also available.

**ONLINE SAFETY TRAINING AT YOUR SCHOOL**

“All teaching and non-teaching staff receive regular and up-to-date training.”

Recommendation from Inspecting E-Safety, Ofsted, January 2014

E-Safety is a whole school issue, not the sole responsibility of the ICT Co-ordinator. Keeping young people safe online should be part of everyone’s job. “E-Safety [should be] comprehensive and threaded though the school.” Ofsted, Inspecting E-Safety September 2012

E2BN provides INSET sessions for staff that address a range of E-Safety issues. For more details on the E2BN online safety training in school, contact Kathy@e2bn.org she will be delighted to discuss your particular online safety training needs.

**Details of the courses available follow on page 06**
Teaching Digital: This session is designed to encourage staff to think about how online safety education can be incorporated into a variety of subject areas and starts off with a quick look at web filtering. Why do we need it and what should the smart teacher need to know about managing it? The web as a research tool and issues of evaluation and copyright and questions why we are teaching children to steal. The need to teach children to think before they post, issues around grooming, cyberbullying and the impact of a negative digital footprint have those staff involved in PSHE, pastoral care and careers education really taken note? And because we wouldn’t want PE, drama, dance or music teachers to feel that this stuff doesn’t have anything to do with them, there’s a great video showing that it does! In case anyone still thinks online safety isn’t part of their job, we take a quick look at setting a good ‘e-example’, data security, Acceptable Use Policies (AUP) and what Ofsted have to say about all this.

Online Professional Reputation for Staff: This presentation is designed to encourage all school staff (including non-teaching staff) to consider how their online behaviour could impact on their real world professional reputation. Although the focus of the session is staff behaviour, it carries powerful messages about what we should be teaching about the online world. We will explain what is meant by digital tattoo, raise questions about what is right, wrong, normal and acceptable online, address issues around cyber-vetting and give suggestions about how to build a positive online reputation. As a final thought, staff are asked to consider whether the school’s current AUP provides them with enough guidance and the school with enough protection.

Managing Sexting Incidents in Your Primary School: It is tempting to think that ‘this sort of thing’ only happens amongst teenagers. Unfortunately, children as young as six have been involved in sexting. Whilst young children may well sext for ‘fun’ or to entertain their friends, it is extremely likely that such behaviour will still be dealt with by the incident. But do you know what to do? Are you sure that you (and your staff) know if and when you should report to the police or social services? Have you thought about how to advise parents and what, if anything, to teach pupils about sexting? This 90 minutes will help you and your colleagues make the right decisions.

Online Safety for Governors: Governing bodies are now required to approve and review the effectiveness of online safety policies and practices. Together with the SLT and DSL, they have shared responsibility for how online safety is managed and implemented, for the creation of a positive safeguarding culture and ethos and for ensuring that all staff are adequately trained in all aspects of safeguarding including online safety. How do you review a policy if you don’t understand online safety? How do you ensure that staff are adequately trained if you don’t know what they need to know? This workshop will help governors understand their role and responsibility for online staff, enable them to make better judgements about the standard of online safety in their school and empower them to keep pupils and staff safe online.

---

General Data Protection Regulation

The New Data Protection Laws and Your School

On August 7th, the government announced its Data Protection Bill which will bring the European General Data Protection Regulation (GDPR) into UK law. In this article, we outline the GDPR basics and activities for the autumn term.

QUICK FACTS...

What is the GDPR?

The GDPR is a new European Union-wide data protection law that must be adopted by all member states.

Why is it happening?

All organisations processing personal data, including schools, must comply with the law on May 25th 2018. It is not acceptable to be working towards compliance on this date.

Why is it needed?

The law is being updated to align with the ways we all share and process data in today’s digital world.

What is the focus?

The focus of the GDPR is to place the individual, known as the data subject, at the heart of and in control of their personal data.

What are the key differences?

The law places much more responsibility on data handlers to be open and transparent with individuals about the data they collect and hold. They are expected to keep the data as secure as they can and inform the Information Commissioner’s Office (ICO) of a ‘notifiable’ data breach within 72 hours. The rights of individuals have also been increased.

Key terminology

Data subject – the individual whose data you hold

Personal data – any information that can identify a living individual

Data controller – the organisation that decides what data to collect and how to process it

Data processor – an organisation that processes the data on the instruction of the controller

Processing – anything that is done with the data

Data breach – when personal data is lost, shared with or accessed by unauthorised people

Data protection officer (DPO) – the DPO’s role is to inform and advise the school about your compliance obligations. They also monitor compliance and act as the first point of contact for supervisory authorities and data subjects.

---

What are the positives?

GDPR raises the profile of the data we all share and we will all be much more conscious of the personal data trail we leave. Recognising this at a young age can only help pupils to be more in control of their personal data. It is an opportunity for your school to review and update the data it collects, how it is managed and secured as well as train your pupils and staff to be more careful with their data and that of others.

What are the challenges?

For many schools, the GDPR will be a culture change, especially if you aren’t meeting the current Data Protection Act. Common data handling practices such as sending data via unencrypted emails, carrying sensitive data in mark-books or on unencrypted memory sticks, fall short of the GDPR security stipulations and will need updating.
General Data Protection Regulation Contd.

THE SIX DATA PRIVACY PRINCIPLES

The GDPR hangs on the six privacy principles. It is easy to get bogged down in the terminology and detail of the GDPR but remembering these principles will help you focus on its key points.

Data must be:

1. collected in a lawful, fair and transparent way;
2. for a specified use;
3. relevant and limited to what you need;
4. up-to-date and accurate;
5. retained for a reasonable period only; and
6. kept securely.

YOUR JOURNEY TO COMPLIANCE

There is much you can do to prepare for the new regulations and this term should focus on raising staff awareness and understanding what data you collect and process.

RAISING STAFF AWARENESS

Add GDPR to meeting agenda

It is critical that your senior leadership team and governing body understand the implications of the GDPR and begin planning for it now. Ensure it is discussed by adding it to all meeting agenda.

AUDITING YOUR DATA

STEP 1 Identifying the data you collect and process

List what personal data you hold across the school, from staff, pupils and parents. Consider the six principles opposite, where and how securely it is held, how it is collected or processed and who it is shared with. Identify which data you collect yourselves and which you receive from elsewhere, such as via the Common Transfer File (CTF) or from other agencies. Adding a column about how better it can be secured is also helpful.

Ask staff what software and websites they use that gather personal data to map a complete picture across school.

STEP 2 Understanding why you are collecting it

Collecting data fairly and lawfully means you must have a lawful purpose for processing the data and there are six lawful reasons for doing so.

One of the lawful purposes is consent but this doesn’t mean that you need to ask permission for every piece of data you collect or process. Indeed, there are very few circumstances where consent will be the lawful basis for the data you collect. One case where would be photographs that aren’t required for teaching purposes, such as for a school brochure or website.

As you work through your data audit, consider why you are processing each piece of personal data and the basis for doing so, not forgetting that this applies to staff and parental data too.

STEP 3 Identifying special category data

Much of the data you collect is done so to meet statutory obligations, such as the data for statutory returns. The data you collect and process for statutory returns.

Data about race, ethnic origin, genetics, health and biometrics (including finger printing), beliefs such as religion, political opinions and trade union membership and sex life or sexual orientation is classed as sensitive or special category data. Work through your list and identify any such data as the rules for this information are stricter than for other personal data.

STEP 4 Identifying the risk

It is important to understand the risk to the individual and the school if there is a data breach. RAG rating each type of data will help you to prioritise staff training and data security. For example, losing the child protection register is potentially much more devastating compared to an attendance register. Understanding how staff access and use data will support you to identify risky practices.

ADD GDPR TO MEETING AGENDA

RAISING STAFF AWARENESS
How E2BN can help?

E2BN is part of Data Protection Education, a company focussing on preparing and training schools to be GDPR compliant. As always we offer free advice and guidance to all E2BN members. We are also offering awareness training sessions.

GDPR Awareness Sessions

Who should attend?

• Headteachers, SLT and governors
• Business and admin managers
• IT managers
• Any staff who have responsibility for managing data

What’s covered?

• How the GDPR applies to your school
• The implications for your role and others in your school
• Your responsibilities in enabling your school to be compliant
• Understanding the risks around GDPR
• Things you can do now to move towards compliance

For more information or to book places on any of the sessions:

Visit: https://dataprotection.education

Email: info@dataprotection.education

Call on: 0800 0862018

Snap Maps  In June, Snapchat updated its app to include a new feature called Snap Maps. It allows users to show their location on a map which other users can view. There are fears that children can share their location with strangers using the app.

There is the ability to turn on a ‘Ghost Mode’ which enables users to hide their avatar on the map. The process to do this is as follows:

• Open Snapchat and go onto your camera screen
• Pinch the screen or do a zoom out finger motion on the screen and Snap Map will open
• You should see your bitmoji icon on the screen
• To turn on ‘Ghost Mode’, go to the home screen and click on the settings symbol (top right on screen)
• There are also other settings where you can make your bitmoji available to ‘my friends’ or ‘select friends’

Not familiar with Snapchat? Check out: www.lifewire.com/snapchat-trends-3485994

Skout  Skout is a flirting/meet up app which uses your GPS to put you in contact with other people. It uses a ‘shake to chat’ which puts you in touch with a nearby person at random. If you shake your app it will connect you with somebody else who is shaking at the same time. When you connect with a random person, you have a minute of anonymity before your profile is revealed.

You can also virtually travel to other cities to meet new people. Skout has a feature which means that users aged between 13-17 will automatically be placed in a ‘teen section’ which bans private photo sharing and prevents chatting with people less than 100 miles away. However, the app cannot verify people’s real ages and police have highlighted concern that paedophiles can target children by pretending to be a teenager. There is also the worry that teenagers can falsify their age and enter the adult section. There are no privacy settings and parents should monitor closely any child or young person using the app.

Live.me  This is another of the popular video streaming apps which many Primary and Secondary aged children are using.

Views from many parents on Common Sense Media highlight real concerns about this app and parents should monitor children who are using it. See: www.commonsensemedia.org/app-reviews/liveme-live-video-streaming-app-broadcast-chat-share-follow-and-be-a-star

Musical.ly  This is a very popular app with 8-12 year olds. It is a social network for sharing user-generated music videos. You can upload your own videos, remix others’ work, or browse content created by other users and by more famous recording artists. Reported issues include: use of swearing and profanity (many popular music tracks include explicit language - the tracks uploaded on Musical.ly generally aren’t the sanitised ‘radio play’ versions), skimpy clothing and sexually provocative dancing. Basically, if ‘popular’ music artists are singing it, wearing it or twerking it, a child/young person somewhere will be lip-syncing, dressing up and gyrating in that manner. There have been an alarming number of reports of paedophiles exploiting the app to groom children.

Find out more here: www.internetmatters.org/hub/expert-opinion/musical-ly-app-parents-need-know/
Digital Tattoo - How Big is Yours?

Your digital identity, or 'tattoo', is the collection of data about you that is available online. Every time you post a picture, like or tweet something you add to your digital tattoo. Sometimes ‘official’ sources such as the electoral role, online petitions, donation sites and your workplace’s website also add to that digital identity.

For some people, having a digital tattoo is very important. If your work depends on lots of people knowing about you; maybe you are a celebrity or provide freelance consultancy services, then it is easy to find on the Internet. If you are trying to hide from an abusive ex-partner then being all over the Internet would not be good. However, it is significant. What if your tattoo looks like your colleagues, employers, friends, family, children. What’s the worst case scenario? If your Facebook ‘likes’ reveal that you have ‘liked’ 15 different gins in the last month, don’t be surprised when murmurs of your alcohol dependency circulate the PTA!

Whether your digital tattoo matters depends on who you are and, crucially, what your digital tattoo reveals about you to people who matter. Think about what your tattoo looks like to your colleagues, employers, friends, family, children. What’s the worst case scenario? If your Facebook ‘likes’ reveal that you have ‘liked’ 15 different gins in the last month, don’t be surprised when murmurs of your alcohol dependency circulate the PTA!

What to do about an ugly digital tattoo?

1. Start with what you publish. Review your social media accounts. Are you sure that what you share is only seen by your intended audience? Check the privacy settings monthly. Facebook is notorious for changing what your alcohol dependency circulate the PTA!

2. Check all of your aliases and any different forms of your name that you use, i.e. Kate, Kathy and Katherine.

3. Check what your friends and employer publish about you and ask them to remove things that put you at risk, are inaccurate or are unnecessary.

4. Report abusive posts about you to the social media platform.

5. Build a positive digital tattoo to counteract negative items.

6. Contact the Safer Internet Centre Professional Helpline: helpline@saferinternet.org.uk

7. In extreme cases you can exercise your ‘right to be forgotten’. Read this article for more information: https://tinyurl.com/y94ptfja

It’s easy to find out about your tattoo: think about your use of social media and your use of restrictions and privacy settings. Who can see what? Then, Google yourself. Turn Internet detective and see what you can find out. This will give you a good idea of what other people can discover about you.

When you search for yourself online, try a number of different search terms and combinations. Try your name, your name plus where you live, names of significant others, usernames and aliases.

If your name returns lots of results for you associated with a particular activity or organisation, try searching for your name minus the activity or organisation. This will remove most of those sites and might reveal some more obscure results.

Digital Tattoo - How Big is Yours?

What do Teenagers want Parents (and Teachers) to Know?

There’s a lot said these days about how different the lives of 21st century teenagers are compared to the teen years of their parents and grandparents. In many ways it is true. 24/7 access to information, instant communication and exposure to a huge range of (unfiltered) opinions means that today’s teenagers have opportunities and pressures quite unlike that of their forebears. Yet when the UK Internet Safety Centre asked children aged 11 to 18 what they really want their parents to know about their digital lives the answers were, perhaps, not that surprising. In their own words...

1. Understand that the Internet plays an important and positive role in our lives

"[Parents need to understand] that not everywhere on the Internet is so unsafe and which areas are.”

"They need to understand that the Internet and social media play an important part in our kids’ lives.”

2. Understand what we’re going through

"I think that parents need to understand that young children do need to be protected on the Internet, however sometimes a small amount of freedom can aid them in some important life lessons.”

"Parents need to understand trust. Of course every parent trusts their child, but going against them is what makes their children go against them as well.”

"They can’t protect their children all the time and need to let them make their own choices in an adult manner even if it means putting them at risk, giving the child the independence needed for life.”

3. Be sensitive to our feelings and treat us with care

"They need to understand how children may feel if something goes wrong for them.”

"They need to treat their kids with care and respect when something happens online.”

4. Give us some freedom to build trust and independence

"They need to trust their children and realise that things can happen that might not be the best thing in the world but they should just talk it out with their child to gain their child’s trust.”

"That children will make mistakes and they need to guide them through the process of what you could do.”

5. We will make mistakes – but you can guide us through this

"I think that parents need to try and understand their children’s situation more so that they know what they are going through so that they can try and help them better.”

"They need to understand the situation so that they can help more efficiently. They may also misinterpret the situation and scold their child rather than helping and empathising.”

Whilst technology may have changed enormously over the last 30 years young people still want the same things teenagers have always wanted: trust, understanding, freedom to make (and learn) from their mistakes and a guiding hand.
Talking to Parents about Online Safety Contd.

More from Snapchat: Snapstreaking

Snapchat is probably the most popular app with 11-16 year olds, with 25% of all Internet users having downloaded it.

A Snapstreak is achieved when two people send Snaps back and forth on Snapchat for a consecutive number of days. In order to keep a streak going, you’ve got to send a Snap back and forth to a friend within a 24-hour window. And, yes, you’ve got to do it every single day.

And just so that you know where you are with the streak, Snapchat displays your ‘streakcount’ and a flame emoji next to your friend’s name. Special emojis appear when your streak has reached a significant score. An extremely long streak will earn you a mountain emoji. And there’s even a sand timer emoji to remind you to Snap as you approach the 24-hour deadline each day.

Snapchat users can invest a lot of time in keeping a streak going. The longest Snapchat streak was 715 days! At its most harmless it is a form of entertainment but a long streak also carries social value. Streaks are seen as a measure of how good your friendship is, of how popular you are. The more streaks Snapchatting teens have the more socially acceptable they feel.

The question for parents, carers and teachers is, of course, is this something else that we should worry about? For many users, streaking is all good clean fun but it can be stressful. Imagine having to remember to send a text or a picture to someone every day! Even if you are ill, on holiday; every single day!

And teens have reported feeling devastated when a long running streak has failed – if your friend has allowed the streak to fail then maybe they don’t like you any more – it’s a huge social snub. And if you are the one who has failed to send that all important Snap, will your friend think you don’t like them any more? Will they be cross with you for ending the streak? The NSPCC has received a number of calls from children saying that they have been upset by a Snapchat streak. One girl explained that she had no wifi that day so she couldn’t send one to her friend and was scared because she thought her friend might think she didn’t like them any more!

"The Internet is a tremendous resource for learning and creativity but it is important to make sure that children are able to make the most of all it has to offer in a safe way. Keeping children safe online is one of the government’s greatest priorities.”

Internet Safety and Security Minister, Baroness Shields.

Who Should Attend?

We all have a duty to protect those in our care and to protect ourselves, so in many ways the question is ‘who shouldn’t attend?’. Our previous Online Safety events have been attended by:

• Headteachers and SLT members
• Governors
• ICT and other subject teachers
• School staff with responsibility for safeguarding
• Child protection directors from Local Authorities
• ICT providers
• Child protection managers
• Children and youth services managers
• Social workers

Why Should You Attend?

The Internet is completely amazing: we can learn, create and connect - opening up a whole world of exciting possibilities. We at E2BN have been passionate about the benefits of the digital world since first providing schools with Internet access all those years ago. Along with our colleagues at NEN - The National Education Network, we have lead the way in online safety. Our conferences offer critical and essential professional development to anyone who works or volunteers with children and young people.

It is an Ofsted requirement that all staff receive regular updating and training in online safety. The E2BN Annual Online Safety Conference is the perfect opportunity to ensure that you and your colleagues are up to date on the latest threats, trends and statutory guidelines.

E2BN Annual Online Safety Conference
Wednesday 8th November 2017
Online Safety Conference 2017
Critical information for anyone with a specific role in Online Safety

Book your place now
Only £70 for E2BN members
or
£95 per non-member delegate

Wednesday 8th November 2017

The Rufus Centre
Steppingly Road
Flitwick
Bedfordshire
MK45 1AH
(within easy reach of M1)

The conference is aimed at Headteachers, teachers, governors, school staff with responsibility for online safety.

Confirmed speakers include:

The 2 Johns, John Staines and John Woodley. Together they have over 55 years of experience in law enforcement. The majority of their careers have been catching and prosecuting paedophiles.
'Stranger Danger in the 21st Century'

David Tidman, eSafeguarding Expert ICT4C
'Digital Literacy: Taught not Caught'

Simon Finch, SIMFIN. Naace Impact Award Winner ‘For his commitment to ensuring a safe and supportive learning environment for the education sector’
'Gender representations in social media'

Stella James, CEO Gooseberry Planet
'Apps designed to help children to learn online safety through gamification'

Zoe Ross
'The Impact of Social Media on Children's Mental Wellbeing'

WWW.E2BN.ORG