Safe and Responsible Use

How can we best keep young people safe online?
Safe and Responsible Use

HOW CAN WE BEST KEEP YOUNG PEOPLE SAFE ONLINE?

Schools have long had a responsibility to keep pupils safe, and the recommendations from Tanya Byron (2008), Ofsted (2010) and others have emphasised that the best way to do this is through teaching pupils how they can best keep themselves safe. This is perhaps akin to cycling: pupils cycling to school are exposed to risks which could otherwise be avoided, but many see the benefits (independence, for health, environmental, easing road congestion, and so on) as being worth the additional risk, so we then do all we can to mitigate the risks through teaching pupils to cycle well and safely.

The computing curriculum includes the requirement that pupils are taught to keep themselves safe, and indeed goes beyond just teaching ‘online safety’ into teaching pupils how to act respectfully, responsibly and securely when using technology, to know what constitutes inappropriate content, contact or conduct and how to report concerns that they may have.

Including these requirements in the computing programmes of study does not mean that these should only be taught in computing lessons, or that the computing head of department becomes responsible for these things: good practice is to see these as a whole school responsibility, and to embed their teaching across the curriculum, and the life of the school. Within computing, these matters can be addressed very effectively through emphasising these as you teach other topics in computing. A few online safety lessons and an assembly for Safer Internet Day seem less effective than an approach in which safe, responsible and secure practices for the use of technology are taught and followed in all aspects of the school’s life and work.

Stepping back from the risk mitigation approach to online safety and seeing the development of responsible use of technology as just one aspect of values or character education (see, for example, Department for Education [DfE], 2014) may be particularly effective. If, over their time in school, we can help develop a strong sense of moral responsibility and the ‘grit’ necessary to stand up for doing the right thing, our pupils leave us far better at coping with the challenges of adult life, as well as being far less likely to fall prey to the more sinister aspects of the internet and other technology.

What are the risks?

In her 2008 report, Safer children in a digital world, clinical psychologist Prof. Tanya Byron (2008) outlined three broad categories of risk to which young people are exposed through their use of digital technology: content, contact and conduct (see Figure 6.1).

![Figure 6.1 (from Byron, 2008)]

**Content**

Young people are naturally curious and teachers would hope to nurture and develop that innate curiosity, doing what we can to establish a lifelong love of learning in our pupils. However, whilst a previous generation’s curiosity might have led them to look up rude words in a dictionary or encyclopaedia, today’s young people are far more likely to search the words they overhear on Google or Bing. The loss of innocence through exposure to highly graphic depictions of sex or violence is far too prevalent. Schools must have effective filters and monitoring in place to prevent access to inappropriate or harmful material (DfE, 2016), but this in itself does little to mitigate the risk to young people through access to such material outside of school, including on smartphones.

Both Google and Bing have SafeSearch settings which, whilst not infallible, will do much to prevent pupils accessing particularly inappropriate content via these; these settings can be locked in place, and
Safe and Responsible Use

a number of organisations have developed search engines targeted at children, often through using a combination of SafeSearch and custom search tools in Google search. Linking this to the computer science side of the curriculum, pupils might consider how algorithms can be designed to filter search results as effectively as they do\(^{(1)}\).

It would be wrong to think of filtering merely in terms of preventing access to inappropriate or harmful sexual content. Schools have a duty to promote fundamental British values and should prevent access to terrorist or extremist material which might lead to pupils’ radicalisation (DfE, 2014, 2015).

Just as schools typically receive a filtered internet connection, in which access to content considered inappropriate is blocked, so parents can request filtered internet access at home and on mobile devices: it’s worth teachers explaining to parents how to do this, and the reasons why they should. Even with filters in place, young people may still encounter content that concerns them, and establishing a ‘no blame’ culture in which they can alert you or their parents to such content can be helpful. Many schools operate a policy of teaching young people to close the laptop, switching off the monitor or turning over the iPad if ever they find content they know they shouldn’t or are otherwise concerned about.

Byron identified other risks associated with content, including commercialisation (qv Bailey, 2011). When teaching pupils about the internet, and particularly the web, it’s worth helping them to become more discerning and critical about commercial aspects of this. These include prevalence of spam in email, how this can be filtered semi-automatically, as well perhaps as what sort of algorithms might be used in doing so\(^{(2)}\). It’s also worth helping pupils to become aware of the use of advertising on the web and how this can be avoided through the use of browser plugins such as AdBlock, as well as the difference between sponsored and other results in search engines. It’s important to help pupils become aware of the difference between altruistically-created content such as Wikipedia, many blogs and much of YouTube, content created with a perhaps hidden or implicit commercial purpose, and the absence of a ‘free lunch’ in many apparently free online services.

Contact

Much good work has been done to teach young people about the dangers of posting personal information online and of contact via the internet from those they don’t already know. Child Exploitation and Online Protection Centre (CEOP) makes some excellent resources available to support teachers in effectively delivering a clear message to pupils about these risks and what they can do to minimise them\(^{(3)}\).

Teachers and parents can do much to help young people become more discerning in their use of the internet or other communication technologies, thinking carefully about strange or otherwise unanticipated contact or communication, and the potential long-term consequence of sharing information online.

‘Sexting’, the sharing of sexually explicit text, images or video via smartphones, perhaps using apps such as Snapchat, seems increasingly prevalent amongst some groups of young people. This is in part due to peer pressure, but also through short-term perspectives and some misconceptions about online privacy. It can have profound consequences for both the sender and recipient of the content. The advice from Childline if someone keeps asking a young person for inappropriate photos is:

- Ask them to stop … or just don’t reply at all and hopefully they will get the hint. But if they are still bothering you or making you feel upset it’s okay to block them — even if it’s just for a bit.
- If an adult has been making you feel uncomfortable by asking you to send them images, you can report them on the CEOP site. If an adult does this it is sometimes called online grooming.
- It is wrong for anyone to be pressuring you in this way. If you are under 18, they are breaking the law\(^{(4)}\).

Whilst acknowledging that it’s illegal for a person under 18 to take or share indecent images

---

3. [www.ceop.police.uk/](http://www.ceop.police.uk/)
4. [www.childline.org.uk/explore/onlinesafety/Pages/Sexting.aspx](http://www.childline.org.uk/explore/onlinesafety/Pages/Sexting.aspx)
Safe and Responsible Use of themselves, current ACPO (Association of Chief Police Officers) advice does not support prosecution, and emphasises the need to put safeguarding at the heart of any intervention.\(^5\)

As with any safeguarding issue in school, teachers have a responsibility to report concerns to the designated person, in accordance with school policies.

**Conduct**

The curriculum requires that pupils understand how to use technology responsibly and respectfully. Supporting young people’s moral development is a vital part of secondary education, a statutory requirement for a school’s curriculum and, as part of ‘spiritual, moral, social and cultural development’, an element of all Ofsted inspections. Kohlberg’s stages of moral development (for example, Kohlberg, 1984) offers one model for thinking about this:

1. obedience and punishment orientation (how can I avoid punishment?);
2. self-interest orientation (what’s in it for me?);
3. interpersonal accord and conformity (the good boy/girl attitude);
4. authority and social-order maintaining orientation (law and order morality);
5. social contract orientation (do unto others…);
6. universal ethical principles (principled conscience).

Under this model, we would hope to see pupils already taking responsibility for their own moral and ethical decisions and behaviour when they get to secondary school, but then supporting them as they learn to do the right thing out of a respect for others and, ultimately, on the basis of their personal adoption of universal ethical principles, probably including such ‘fundamental British values’ as ‘democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs’. If schools take moral education, focussing on character and values, seriously, many aspects of pupils’ inappropriate conduct using technology can perhaps be avoided, or their consequences reduced.

In many schools, **cyber-bullying** is a common problem: a BBC/Comres survey reported 22 per cent of 10–12-year-olds had experienced bullying or ‘trolling’.\(^6\) Whilst this is more likely to happen outside of school, it’s common for both bully and victim to be members of the same class, year group or school, and the cause and consequences may often be connected to school. As with bullying in general, a focus on moral education might reduce the prevalence of such hurtful behaviour in the school community, but a clear zero tolerance message is essential, together with a culture in which this can be reported in the knowledge that swift and effective action will follow. Alongside this, it’s worth building up young people’s resilience to off-hand, unintentionally hurtful remarks from others, and some recognition that not every online disagreement or critical comment constitutes bullying.

**Copyright**, and other aspects of intellectual property, is another area in which young people’s (and sometimes teachers’) conduct isn’t all that it could be. Perhaps because the web works through automatically making copies of the content from a distant web server in the user’s web browser when the page is accessed, and the ease with which digital content can be perfectly copied, it’s all too easy to assume that content found online can be used wherever and however someone wants, without paying attention to the legal and ethical aspects of intellectual property. There are generous exemptions from much copyright legislation for clearly specified educational use,\(^7\) as well as educational use licences for a range a media purchased centrally by the DfE on behalf of state-funded schools in England.\(^8\) It remains important to teach and show best practice in the use of copyrighted material, including properly acknowledging the source of content and respecting any associated licence terms.

The Creative Commons family of licences makes it easy for those who create work in any medium to licence it for re-use, under a range of different conditions; you can teach pupils about this approach

---

\(^5\) [https://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf](https://ceop.police.uk/Documents/ceopdocs/externaldocs/ACPO_Lead_position_on_Self_Taken_Images.pdf)

\(^6\) [www.bbc.co.uk/news/education-35524429](www.bbc.co.uk/news/education-35524429)


\(^8\) [www.copyrightandschools.org/](www.copyrightandschools.org/)
to sharing online, and show them how they can search for, acknowledge and re-use Creative Commons licensed content in their own work. Both Google and Bing image search allow results to be filtered to show just images that have been licensed in this way.

Furthermore, the work uploaded to the Scratch website is covered by a Creative Commons by-share alike licence, as are resources shared on the CAS (Computing At School) community site, except where stated otherwise. There's ample scope in the curriculum for pupils to make use of Creative Commons and public domain content: the Key Stage 3 programme of study requires that students are taught to ‘reuse, revise and repurpose digital artefacts’ – and artefacts produced by others but available online under liberal licenses would work well for such activities.

It’s worth bearing in mind that pupils automatically own the copyright in their own work, including that which they produce in school, and that we as teachers should respect this, for example checking with pupils and their parents before publishing their work online in a class or school blog. Asking parents to licence these and similar uses by the school of their children’s work might seem unnecessarily legalistic, but it’s important that pupils learn about, and have respect shown for, their rights as well as their responsibilities.

It’s important that pupils be taught to respect the terms and conditions of any websites or other online services which they use, and indeed see you doing so yourself. The terms and conditions of most online services run to many, many pages, but when signing up for new services or asking pupils to do so it’s well worth checking through the sections on any age-restrictions as well as those on copyright and data privacy. US-based companies are required to abide by American COPPA (children’s online privacy protection rule) legislation, which prevents their storing personal data on under 13s without parental consent. As a result, many US-based internet services and websites (including Facebook) prohibit under 13s from creating accounts or using the service. Pupils under 13 using these services would be doing so without the operator’s permission, which could be considered an offence under the Computer Misuse Act.

A number of services, including Google Apps for Education and Office 365, allow schools to create accounts on behalf of children, with the school taking responsibility for obtaining the necessary parental consent. Other websites, such as Scratch, allow teachers to create multiple accounts in their own name and share these with pupils but this is an exception rather than the rule: it’s much better to check, and abide by, the terms and conditions rather than making these assumptions.

Concern is sometimes expressed that young people might use their knowledge of programming and computer networks for harmful or illegal purposes, including cybercrime. Even in the context of school networks, it’s not unheard of for pupils to attempt to obtain administrator or teacher password details, bypass filtering through proxy servers or VPNs (virtual private networks) or attempt to install keyloggers or password sniffers: all of these are likely to be prohibited under the school’s acceptable use policy. Pupils investigating the tools and techniques involved here may get drawn in further to a subculture in which circumventing computer security is seen as an acceptable intellectual challenge.

The Computer Misuse Act was introduced to make hacking computer systems illegal. It covers a number of offences involving the unauthorised use of computers, with or without the intention of committing further crimes, or impairing the operation of computers. As well as account hacking, using malware including rootkits is against the law, as is conducting distributed denial of service attacks. The National Crime Agency suggest a number of warning signs that parents might watch out for to alert them to a young person’s involvement in cybercrime:

---

9 That is, content which can be used without any restriction, sometimes called Creative Commons 0.
Safe and Responsible Use

• Are they resistant when asked what they do online?
• Do they get an income from their online activities, do you know why and how?
• Is your child spending all of their time online?
• Do they have irregular sleeping patterns?
• Have they become more socially isolated?

Whilst parents of many teenagers not involved in cybercrime might answer yes to many or all of these, it’s important that parents and teachers feel able to discuss any concerns or suspicions they have over an individual’s interest in or involvement with criminal activities. A clear emphasis on character or values education in school, including in computing lessons, might do much to help prevent young people becoming involved in computer-based crime.

Finally, be aware, and make your pupils aware, of the opportunity cost associated with screen time – time spent using a computer, tablet or smartphone is time not spent doing other things, such as reading a (paper-based) book, learning a musical instrument, playing in a team and socialising face to face with family and friends. Whilst digital technology is seen by many as transformative of so many aspects of learning and life, many would count it a great shame if it came to dominate childhood, within or beyond school, to any greater extent than it already has. Helping young people to become more discerning users of technology, knowing when it would be useful, and when it might be more of a distraction, is perhaps also one of our responsibilities as teachers.

The new curriculum requires that pupils are taught how to report concerns they have over technology. In most cases, pupils should talk to their parents or their teachers about such concerns: if pupils report such concerns to you, this may be covered by your safeguarding policy, so make sure you follow this very carefully. Sometimes, pupils might be too embarrassed about something to turn to either you or their parents so it’s worth making them aware that there are others who can they talk to, including Childline and CEOP.

Pupils need not be directly affected by something to report it: it’s important to establish a classroom and school culture in which pupils feel that they can discuss any concerns openly with teachers and one another, including if they believe any of their friends are involved in risky online activity or if they notice unusual changes in their friend’s behaviour. A number of schools have established a ‘digital leader’ role for pupils, which might include particular responsibilities around supporting other pupils in staying safe online.

Older pupils should also know how they can address concerns they have, particularly over content or conduct, with social media sites directly. And reputable sites, including Facebook, Twitter, Tumblr, Instagram and YouTube, will act promptly in the case of illegal activity or where the site’s terms and conditions have been infringed.

Classroom activity ideas

● Online safety and responsibility provide great topics in which pupils can develop their creative use of technology. From making and giving high-quality presentations and blogging advice for younger pupils to creating short live action video or animations exploring these issues, there’s ample scope here for pupils to work collaboratively and produce high-quality work across a range of digital media.

● Pupils might work together to develop a website summarising the terms and conditions, and reporting arrangements, for popular social media platforms and apps.

● Keep abreast of media stories concerning illegal or unethical use of technologies, using these as starting points for class discussions. Encourage pupils to use a framework of ethical principles when discussing these.

12 www.childnet.com/new-for-schools/childnet-digital-leaders-programme
13 See www.thinkuknow.co.uk/14_plus/help/Contact-social-sites/ for links to policies and reporting portals for many social media providers.
14 Pupils might enter their film for Childnet’s annual competition: www.childnet.com/resources/film-competition/
Online content, conduct and contact issues might be effectively explored through role-play and discussion, although you should be aware that some pupils might be directly affected by some of these issues and thus a particularly sensitive approach may be necessary. Dilemma cards might be particularly useful.

Further resources


Creative Commons (n.d.) For information and free licences to use. Available from http://creativecommons.org/


Thinkuknow.co.uk (CEOP) (n.d.) Resources for lower secondary pupils. Available from www.thinkuknow.co.uk/11_13/; and for teachers: www.thinkuknow.co.uk/Teachers/

UK Safer Internet Centre (n.d.) Available from www.saferinternet.org.uk


Privacy, Security and Identity

Online safety is linked directly with issues of privacy, security and identity, and these topics lend themselves to further exploration within computing lessons. Privacy and security are closely-related ideas but are not synonymous: we put curtains at our windows to protect our privacy but fit locks to our doors to maintain security.

Privacy

Pupils in Key Stage 1 are taught that they should keep personal information private. In Key Stage 3 they learn how to use technology to protect their privacy.

Pupils ought to have a good idea of what’s meant by personal information. The Data Protection Act defines personal data as data about a person who can be identified from the data. This includes names, home addresses, personal phone numbers and email addresses, as well as photographs or videos showing the face of a person, but it might also be reasonably seen as including the Internet Protocol (IP) or Media Access Control (MAC) addresses of connections or computers used by the person or details of their social media accounts.

15 https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/
There’s other information which a person might reasonably expect to be kept private, such as their internet history, their search history, mobile cell or Global Positioning System (GPS) location information, personal photographs and records of mobile phone calls or email correspondence.

Keeping all this information entirely private is, to all intents, incompatible with the use of online technology – when using a standard mobile phone, the network operator must know the cell to which any call should be routed; when communicating by email, the email provider of sender and recipient must have access to the email and its contents; search providers must know what it is that you are searching for if they are to provide results; web servers automatically maintain records of pages requested and the IP address of the computer requesting them: such information has to be provided through the very nature of the technology used. Similarly, without encryption there’s nothing to prevent routers, gateways and switches sniffing the contents of the packets transmitted through them across the internet’s infrastructure. Users particularly concerned about privacy issues might set up their own virtual private network, (16) use an anonymising routing protocol such as TOR, (17) set up their own server and domain for email and other services, (18) and avoid social media: for users outside of oppressive regimes, such steps might suggest an excessive degree of paranoia or that they have something to hide.

Rather than such an entirely paranoid approach, it’s worth getting pupils to think in terms of circles of trust, thinking carefully about with whom they would choose to share information. There are some people whom a pupil should trust to a very great extent, secure in the knowledge that that person has the pupil’s own best interests at heart: one would hope that for almost all children this would include their parents and their teachers. With those in this circle of trust, pupils might confidently share almost any information. Close friends and relatives might be trusted somewhat less, but we would be predisposed to consider them worthy of our trust in most matters. There’s then a looser circle of friends and acquaintances, who we are perhaps somewhat more wary of, but still willing to invest some trust in to strengthen such relationships although we might exercise some degree of caution in doing so.

In a benign, liberal democracy, and in an education system which placed its pupils’ well-being as its number one concern, we might also consider the police, other government agencies and those maintaining the security of the school’s information systems as meriting a high degree of trust, although not all would necessarily agree.

Many of us feel confident placing our trust in large, multinational corporations, not because we believe they act in our best interests but because what they provide in return for what they ask seems a good deal, and many such organisations have stated policies in which they seem to take their customers’ privacy very seriously, even if on their own terms rather than ours.

Those who we don’t know are another matter. Back in Jane Austen’s day, new acquaintances would only be accepted once they had been introduced, either by letter or in person, by someone already known and trusted and perhaps something similar operates, at a lower level of trust on the web and through social media.

It seems clear that some degree of caution and discernment are needed when navigating the complex web of personal, commercial and regulatory relationships that our online life makes us part of. To share nothing of oneself denies the opportunity for participation, to share everything seems foolhardy: a middle path in which we share those things which we can trust the other with, with those others whom we trust, whilst keeping to ourselves and a closer circle those things we would rather they did not know seems the appropriate way to strike a balance between these extremes.

In sharing information online, pupils should be aware of the long-term persistence of the information they share – what goes online typically stays online. Once a photograph, video or message is available on the open web, then anyone with access to it may be able to make a copy of it – indeed the very act of viewing the content involves transferring that content from a web server to a computer. Google’s Page Rank algorithm can only operate through indexing a cached copy of the

16 For example using a Raspberry Pi: www.bbc.co.uk/news/technology-33548728
17 www.torproject.org/
18 Perhaps using https://owncloud.org/ or https://sandstorm.io/
Safe and Responsible Use

web. The Internet Archive similarly makes regular copies of many websites to preserve this content for the future. Even within password-protected sites, it’s essentially impossible to prevent what other users with access to content will do with that content. A photograph might be shared in the expectation that it would remain private but the other person might still, in a breach of trust, share a copy of that with others or on the open web. That which a pupil thinks is worth sharing at the age of 14 might subsequently be regretted when it remains permanently associated.

As well as deciding for themselves with whom to share particular information, based on the extent to which they trust the other, pupils should be aware of the routine and almost inevitable recording or surveillance of their online activities. As mentioned above, schools now have a duty to monitor pupils’ access to the internet; internet service providers maintain records of sites visited; mobile phone companies maintain records of the cell masts to which a mobile phone automatically transmits its location; search engine providers build detailed profiles of users based on their search queries and other activities; social media sites and app providers similarly know much about who any one of us is friends with or follows.

When the investigatory powers bill\(^{(19)}\) becomes law, much of this information would have to be disclosed to investigators in certain defined circumstances. Many would argue that such recording or surveillance is a not unreasonable price to pay for the online services provided and to ensure that individuals and society are protected from those who would wish them harm.

Pupils should have a reasonable expectation that any data held about them is kept private, as the Data Protection Act\(^{(20)}\) requires. That personal information is not, without one of a few very good reasons, or the subject’s explicit permission, shared with third parties, and that when others are, of necessity, involved in processing data they too have an obligation to protect the privacy of those to whom it relates. This expectation applies to schools as much as to any other organisation processing personal data, and includes the expectation that data be kept securely, in such a way that unauthorised users cannot access it.

---

Security

Security is about preventing those who shouldn’t have access to data, information or systems from gaining access to that data, information or systems.

Security is related to privacy – in general it’s a necessary but not sufficient condition, that is, you cannot expect privacy without security, but privacy needs more than just security.

At one level information can be kept secure by physical means – recording information on paper only and storing that information in a safe or locked filing cabinet would foil all but the most intrepid.\(^{(21)}\)

On a computer, an ‘air gapped’ machine\(^{(22)}\) without network access and without support for removal media would provide a high degree of security for any data stored on it, assuming that the physical security of the system itself could be guaranteed, although it would be a far from convenient system to use for most practical tasks.

Beyond the physical security of a system, some attention should be given to the security of the data stored on it, or on removable media used with it – whilst challenge and response passwords provide a degree of protection, encrypting the data is the best way to ensure that even if unauthorised users gain access to the system or find the memory stick, it would be essentially impossible for them to read the data stored on the device without knowing the secret key with which the data had been encrypted. These days, most operating systems include the ability to encrypt all of the data on the startup disk or equivalent system, and communication via the internet can be routinely encrypted without any additional efforts. Smartphones can be set to delete any data stored on them if a wrong passcode is entered more than a set number of times, and can be wiped remotely when connected to the internet.

---

21 See, for example, [www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance](http://www.theguardian.com/world/2014/jul/15/germany-typewriters-espionage-nsa-spying-surveillance)
Cryptography

Cryptography is central to an understanding of the security of digital data, and particularly to its communication via the internet, over what are essentially insecure, open channels. The encryption techniques used to transmit messages securely can also be used to store those messages securely too.

In classical cryptography, we take a plain text message to be encrypted, some agreed protocol for encrypting the message and, crucially, a secret key that’s used to encrypt the message into some ciphertext. The idea is that, even if the enemy has access to the ciphertext and full knowledge of the protocol used, they cannot recover the original plain text without knowing (or guessing) the encryption key used.

Figure 6.3 Image of Caesar cipher wheel: this from https://commons.wikimedia.org/wiki/File:CipherDisk2000.jpg

The history of cryptography is a long and interesting one. One of the earliest cryptographic systems was the Caesar cipher, in which the letters in the plain text message were simply shifted along the alphabet by an agreed number of places – thus the plain text

attack at dawn

would become the ciphertext

BUUBDL BU EBXO

Decrypting the message is simply the reverse of this process, shifting each letter of the ciphertext back along the alphabet the correct number of places.

Whilst this is an easy system to implement by hand and to code on a computer, it’s very far from secure: to break the encryption the enemy only needs to try the 25 possible shifts until something in English turns up.

A more sophisticated system might involve replacing each letter in the plain text alphabet with an agreed letter in the cost text alphabet, for example, we might swap

\[a b c d e f g h i j k l m n o p q r s t u v w x y z] \quad \text{with} \quad \text{E G L J H O T U P V F S X A W Q K R M Z D Y N C I B}

Using this key, the message

attack at dawn

would become the ciphertext

EZZELF EZ JENA

With knowledge of the key, this is reasonably easy to decipher by hand, and easy enough to program on a computer (Figure 6.3).

```python
def encode(message, cipher, plain="abcdefghijklmnopqrstuvwxyz"):
    ciphertext = ""
    for i in range(len(message)):
        letter = message[i]
        position = plain.find(letter)
        ciphertext += cipher[position]
    return ciphertext
```

Figure 6.4
Safe and Responsible Use

if position > -1:
    ciphertext = ciphertext + cipher[position
else:
    ciphertext = ciphertext + " "
return ciphertext

Simple substitution functions in Snap! and Python

At first sight, it looks very hard to break by trying out all the possible key combinations (of which there are $26 \times 25 \times 24 \times \ldots \times 2 \times 1$ possible keys, roughly $4 \times 10^{26}$), but such brute force approaches are only ever the last resort of cryptanalysts or hackers. If the language of the original message is known or can be guessed, and the message is long enough for statistical techniques to work, then the enemy can use the relative frequency of letters (and pairs of letters) in the original language to start making plausible guesses of which letter had been swapped for which (see the discussion of Shannon and information entropy on pages 92 - 94). For example E and T are the most common letters in English, T is more likely to be followed by H than any other letter and so on. Unsurprisingly it is possible to automate or at least semi-automate this frequency analysis approach to breaking a simple substitution cipher. Automated or semi-automated breaking of codes has figured prominently in the history of computing, most notably in the work of Turing, Flowers, Welchman and others at Bletchley Park in the Second World War.

A more sophisticated system still is the Vigenère or polyalphabetic cipher in which different Caesar shift covers are applied to different letters of the plain text according to some predefined system. For example, one could take the letters of a key word and use these to determine different Caesar shifts: the key word FAB could suggest shifts of 6, 1 and 3 positions repeatedly, or a longer text, such as an agreed passage from a book could be used. This is far less amenable to frequency analysis.

def vigenere(message, key):
    ciphertext = ""
    for i in range(len(message)):
        letter = message[i]
        newletter = (ord(letter) - 96 + ord(key[i %
len(key)]) - 96) % 26
        ciphertext = ciphertext + chr(newletter +
64)
    return ciphertext

Simple implementation of a Vigenere or polyalphabetic cipher in Python

Such a system can form the basis of an unbreakable code – a ‘one time pad’ (Shannon, 1949) in which Caesar shifts or their equivalents are applied according to a genuinely random stream of values known only to sender and recipient in advance of communication. If there’s no pattern to the shifts that are applied and if the random stream is known only to sender and recipient then even a brute force attack cannot recover the original plain text, as all information about the plain text is hidden within the randomness of the key. The downside is that the key must be the same length as the plain text and cannot be used again – hence the ‘one time’ name for this method. Furthermore, the security of the communication now becomes about marinating the security of the one time pad, which is at least as hard as marinating the security of the message it was designed to protect.

Figure 6.5 One time pad

PD: https://upload.wikimedia.org/wikipedia/commons/thumb/6/62/One-Time_Pads_-__Flickr_-__The_Central_Intelligence_Agency.jpg/399px-One-Time_Pads_-__Flickr_-__The_Central_Intelligence_Agency.jpg
Whilst the one time pad is secure, it is impractical for general-purpose communication on the internet, due to the key exchange problem. If Alice and Bob are to communicate securely, they need to agree in advance the key they will use, and this would need to be communicated securely — and if Alice and Bob can do this already, they have no need to establish a new secure communication channel…

The breakthrough to the key exchange problem came through finding mathematical functions which were easy to perform but very hard to reverse. For example if I take two very large prime numbers it’s easy to multiply them together, however, given the product of two very large prime numbers, it’s very hard, even for a very fast computer, to reverse the factorisation. Without the aid of a calculator, you should be able to multiply 7,919 and 8,863, but even with a calculator it would take a long time for you to find the factors of 62,080,727. Factoring this number is relatively trivial but finding the factor of a number some 620 digits seems beyond the reach of even the fastest computers for some time to come.

There’s a little more to Diffie-Hellman (see Diffie and Hellman, 1976; and also Merkle, 1978) key exchange than simply multiplying large prime numbers together. But the idea here is that it allows two people to communicate to decide a secret key that could be used for encryption using another cryptographic system, in such a way that anyone eavesdropping the communication about the key couldn’t work out the key, because it relies on secret information that is never shared. Thus, when communicating over the internet, my browser and the server it is communicating with can, across an open channel, establish a secret key known only to them and then use this for subsequent encrypted communication — without the key itself ever being transmitted, and in such a way that no third party can guess that key.

Another approach to the key exchange problem, again based on the difficulty of factoring a product of primes compared to the ease with which they can be multiplied, is the RSA public / private key algorithm. Here two different keys are needed for the cryptographic system, one which allows data to be encrypted, the public key, and another which allows a message to be decrypted, the private key. If I wish to encourage folks to communicate with me securely, I can publish my public key on the web and invite anyone to use it. Folks can then send me encrypted messages using this key, but even with access to the public key no eavesdropper can reverse the encryption process to read the message, as this is only possible using the associated private key, which only I have access to. RSA offers another advantage in that it allows me to cryptographically sign messages — I could, for example encrypt an outbound message using my private key; anyone reading this could then decrypt it using my public key, and the fact that it can be decrypted using my public key proves that it was originally encrypted (that is, signed) using the associated private key that only I hold.

The HTTPS protocol used for secure communication for web traffic over the internet builds on these ideas. HTTPS does two things: it establishes that the computer you are talking to is who you think you are talking to, by presenting (and checking) a signed cryptographic certificate and it sets up secure communication for subsequent communication between you and the far web server. Thus when I visit my bank’s home page over HTTPS, my browser checks that the site carries a cryptographic certificate signed by someone I already trust (one of a number of supposed incorruptible certificate authorities accepted by my browser); assuming all is well, key exchange for the session takes place and all the following communication, from my password through my statement to setting up new payments is done in secret, even though this is over the insecure channels of the internet.

HTTPS has vulnerabilities, but it’s not vulnerable to folk in the same coffee shop sniffing otherwise open or poorly-encrypted WiFi traffic. The vulnerability lies in the acceptance of certificate authorities (Callegati et al., 2009) — on a school network you may be expected to accept, to trust, a security certificate from the school for internet access. Once you’ve done so, it’s possible for the school’s gateway computer or router to sit between you and distant web servers (a man-in-the-middle attach) routinely decrypting and re-encrypting any traffic between you whilst assuring you that all is very well as you’ve trusted it to sign and to encrypt traffic on your behalf. Were it not for this, and assuming HTTPS access is permitted, it would be possible for pupils to use HTTPS to access web-based content in school without the school being able to monitor or filter what they were accessing.

As well as encryption of data and communication, it's worth considering some other elements of security.

As well as ensuring that unauthorised users cannot access data, it's important for the security of data that those who should have access do have access, even if disaster strikes. In part, this involves implementing a robust approach to backing up and archiving data. In the case of data stored locally on hard drives or removable media a sensible approach would be to make copies of this at regular intervals, wherever possible ensuring this happens automatically, thus protecting against hardware failure of a drive or memory stick, and, in some cases, against operator error too. It's wise to store one copy of the data in another location, to protect against fire or theft. If the capacity and availability of backup media isn't an issue, then an incremental backup policy is wise, keeping older copies of data as well as recording subsequent changes, thus allowing older versions of files to be retrieved if subsequent changes harm their integrity.

In the case of data stored 'in the cloud' on remote servers, it's important to establish whose responsibility it is to backup data. Google, Microsoft and other reputable providers will have robust and well-tested backup strategies in place and you might consider using a service such as this as an additional backup for locally-stored files. For sensitive data you should consider encrypting such files locally before storing them remotely.

It's particularly important to protect the integrity of any admin or root accounts on a computer or particularly a server or domain. Such accounts should not normally be used when operating the computer at a user level, as it's possible for accounts with these privileges to make far reaching and long lasting changes to other users' data and the system itself. You should take particular care if installing software using these accounts that any programs installed come from a trusted source.

Pupils construct their identity in many ways, often presenting different persona in different contexts, behaving quite differently at school, at home and when out with their friends. Online identity can make this harder as multiple accounts across different services are often linked, either explicitly or implicitly. Many social media sites, most notably Facebook, prohibit multiple accounts and require that one registers using a real name. Furthermore open platforms and an eagerness to share content can make it hard for young people to maintain different persona in different online contexts. Both the deliberately shared and the automatically recorded aspects of a digital footprint become inextricably linked to a user's online identity. Young people, and their teachers, can do much to promote their best selves to the world online, and some recognition of the persistence of online data and their responsibilities might encourage them to do so. This is less about using the web to experiment with the cybeculture (Turkle, 1995) of the past as it is about presenting an authentic picture of one's best self.

As more and more aspects of pupils' learning and life are mediated through online systems, it's important that they learn to protect their own online identity and respect the online identity of others.

Typically, online identity is established through some form of password system. Pupils should treat passwords as they do toothbrushes: only use their own, and change them regularly. Encourage pupils to use long passwords that cannot easily be guessed (for example CorrectHorseBatteryStaple, 24 or in accordance with the rules enforced on the systems they access), to use different passwords for different sites or services, and to change passwords regularly.
Discourage pupils from sharing passwords with one another as this is usually their only way to prove who they are in any online system, and avoid encouraging pupils to share their passwords with their parents: many difficulties could arise through one parent impersonating their son or daughter in an otherwise secure ‘walled garden’ environment such as a school VLE or learning platform. Remind pupils that they should log off when they have finished using a computer or website, and that they should only allow browsers to maintain logged-in status if they are the only person with access to that browser. Similarly they should only ever use the ‘remember my password’ feature in a web browser if they are certain that they are the only person who will use that browser. Pupils should consider which accounts they care particularly about and ensure that passwords for these are unique and particularly secure, for example a main, personal email account should always have a unique password since it would be the principal means of requesting a password reset for other online accounts.

Encourage pupils to consider the security of their passwords on the server they are connecting to. There have been well-publicised stories of user account databases being hacked and passwords sold on, which is particularly worrying for users who happen to have used the same password across multiple sites. Passwords should never be transmitted in an unencrypted form. A secure password system must never store the password itself in an unencrypted form, and it should never be possible for those who maintain the system to recover the original password: distrust (and stop using) any system which, when you ask for a password reminder, is able to tell you what password you set.

Figure 6.6 From XKCD at https://xkcd.com/936/, licenced CC by-nc
When setting a password online, the minimum acceptable approach would be for the browser to transmit the password via an encrypted connection, then for the server to cryptographically ‘hash’ the password and store this hash in the database. To check the password, the user transmits their password over an encrypted connection; this is again hashed by the server and the hash compared to the stored version. If they match, the user can access the system. This system too is vulnerable if the password table is available to an attacker, as possible passwords can simply be hashed and compared to the hashed value in the table. By adding some predetermined, unique, random ‘salt’ to the password before it’s hashed the risk here can be mitigated.\(^{25}\)

For particularly sensitive accounts consider some form of two-factor authentication. User authentication can be based on who a person is, what they know or what they have. Usual password protocols rely on one factor only: what a person knows. Simple swipe cards or biometric systems sometimes used for registration, catering or library access rely on what a person has or who a person is. Two-factor systems require two distinct elements before allowing access. For example an ATM uses a relatively insecure four-digit PIN because it only provides account access if the user has the corresponding card. Online systems which send authentication codes to mobile phones or require codes to be generated on a previously authenticated app or device provide a similar degree of security – even if an attacker guesses the account password, they cannot get access without also having the associated phone. If the phone used can only be unlocked with a fingerprint or biometric then this could be considered a three-factor authentication system.

Any such authentication systems are vulnerable if users can be tricked into giving away their passwords, and it’s important to teach pupils how to spot phishing or other social engineering attempts. For example, pupils should learn to distrust the links shown in emails or similar messages as these can be spoofed and point to websites other than those suggested. Pupils should never give passwords out in response to questions, whether online, face to face or by phone.

Classroom activity ideas

- Help pupils to consider the extent of their digital footprint, perhaps keeping a diary of the apps they use in one day or reviewing their own browser or search histories for a day. Take care here as some pupils might be particularly sensitive to the associated issues around privacy and surveillance. What do pupils find if they type their name into Google? Ask pupils to review their privacy settings on any social media sites they use. If they have accounts for services they no longer use, why don’t they delete them?

- A combined visit to the birthplace of computing\(^{26}\) and the home of wartime codebreaking efforts\(^{27}\) is highly recommended, although places for school visits tend to be booked months in advance.

- Talk through some of the issues of privacy and surveillance with pupils. Do they consider this an appropriate way to keep them and others safe? Is it acceptable to use search or browser history or tracking cookies to better target marketing information? Do they mind automated systems reading their emails?

- Cryptography is rich territory for linking pupils computational thinking and programming skills to issues of privacy and security. Can pupils write programs to implement simple cryptography systems in Snap! or Python? Can they write programs which can crack or help crack simple encryption? Can they implement a program to securely store salted and hashed passwords and then check a password against this?

\(^{25}\) See [www.owasp.org/index.php/Authentication_Cheat_Sheet](http://www.owasp.org/index.php/Authentication_Cheat_Sheet) for more details about secure password systems.

\(^{26}\) [www.tnmoc.org/](http://www.tnmoc.org/)

\(^{27}\) [www.bletchleypark.org.uk/](http://www.bletchleypark.org.uk/)
Further resources


Cyber Security Challenge UK (n.d.) Available from https://cybersecuritychallenge.org.uk/


Open Rights Group (n.d.) Available from www.openrightsgroup.org/


References


DfE (2014) Promoting fundamental British values through SMSC.


QuickStart Computing

Key Stage 3 Subject Knowledge covering the Transition from Primary to Secondary

QuickStart Computing provides the vital subject knowledge enhancement for secondary computing teachers.

It covers the content of the Key Stage 3 computing curriculum so that you and your colleagues can teach it confidently and successfully.

Inside you’ll find:

• Detailed coverage of computer science, IT and digital literacy topics included at Key Stage 3
• Guidance on developing and applying the concepts and approaches of computational thinking
• Programming examples using Scratch, Snap! and Python
• Practical, classroom activities and inspiration
• A carefully curated collection of the best online resources and reference materials
• Notes on what’s covered in primary computing to ensure excellent transition

All this guidance is also available online at: computingatschool.org.uk/quickstart

QuickStart Computing for secondary schools is also available at: computingatschool.org.uk/quickstart

Funded by

Computing at School
Educate - Engage - Encourage
Part of BCS, The Chartered Institute for IT

Department for Education
Microsoft