babington

Safe and Sound

Online Safety Handbook

3,205 - Safe and Sound Online Safety Handbook V4 - September 2025

Online Safety Handbook

Contents

Online Safety Handbook

Introduction

Welcome to Babington and the first steps of your learner journey. You will have been made aware that our Apprenticeship delivery in now fully online. Although you won't be accessing our network or equipment, we want to assure you that every precaution is taken to make sure you are safe whilst operating via the online world. Afterall our priority is to keep you Safe and Sound during your time with us here at Babington.

Technology is rapidly evolving, and we all have access to an increasingly wide range of devices and media at our fingertips.

Operating within an online space is something most of us simply do subconsciously, but have you ever stopped to consider the potential dangers which exist on the web.

Being safe online means individuals are protecting ourselves and others from online harms and risks which may jeopardise our personal information, lead to unsafe communications or even effect our mental health and wellbeing.

It goes without saying that the internet can be an unforgiving place. Aside from the more obvious risks such as online bullying, grooming, privacy and identity theft, radicalisation, or device addiction.

The way we are engaging with the online world means that we have to take stock of our mental health and wellbeing, the type of content we are viewing and what we are posting online.

The internet provides you with many ways to stay connected with people at all hours of the day and night, from texts, messenger apps, emails, forums, chatrooms, telephone calls and video conferencing, this online safety booklet will provide you with advice, guidance and tips on how to stay safe online.

Online Safety Handbook

Screen Time

Not all screen-based activities are bad. Being online can be fun, keeps you entertained, it can help you learn and develop new skills and keeps you in touch with friends and family. On average, we spend around 11 hours a day staring at some kind of screen, whether that be a computer, phone, tablet, TV etc. For office workers, some of that is unavoidable, but extra recreational or excessive screen time can impact you negatively also. Like with anything, too much of it can have a negative effect on your wellbeing.

Negative effects of too much screen time

- Excessive screen time can lead to numerous health concerns, including eye strain, headaches, neck, shoulder, & back pain, tendonitis, carpal tunnel & other repetitive-use injuries. It can also lead to Insomnia and poor sleep.
- Social media addiction which can be psychologically detrimental due to more people seeking external validation that leads to depression, mental health concerns and self-confidence issues.

Screen Time Recommendations

There are a few things you can do to reduce the amount of time you spend on an electronic device, or at least to mitigate some of the effects:

- While working on a computer, look away and at a distant object for about 20 seconds, every 20 minutes. Take a quick standing stretch break every hour or learn a few “chair yoga” stretches to keep muscles loose and pay attention to your posture.
- Avoid screen usage before bedtime as it can lead to poor sleep or insomnia.
- No screen time for babies up to 18 months. Ages 18 to 24 months only high-quality media sources and supervise your child’s usage. Ages 2–5 should spend no more than an hour a day on a device. For older kids, you can decide what is okay.

Online Safety Handbook

Privacy and Identity Theft

The internet offers access to a world of products and services, entertainment and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves.

Identity theft is a method used to carry out criminal activity, involving unauthorised use of your name and personal details to either steal from you, or commit a crime in your name. Identity theft can be carried out either online, physically using printed documents, or by a combination of the two.

The Symptoms

- Not receiving bills or other correspondence, may suggest that a criminal has given a different address in place of your own.
- Receiving credit cards which you did not apply for, denial of credit new credit, or unrecognised entries on your credit history.
- Receiving calls from debt collectors or companies about things you have not bought.
- You have recently lost or had stolen important documents such as your passport or driving license.
- You see entries on your bank, credit or store card statement for goods you did not order.
- You cannot log into a site using your normal password (because a criminal has logged in as you and changed it).

Prevention - while identity theft can happen to anyone, there are some things you can do to reduce your risk.

- Do not share account information with friends, family or other people.
- Ensure you always have effective and updated antivirus/antispyware software running.
- If possible, arrange for paperless bills and statements.
- File sensitive documents securely, and shred those you no longer need, preferably with a cross-cut shredder.
- Never divulge private information data in response to an email, text, letter or phone call unless you are certain that the request is from a bona fide source.
- Don’t click on links in emails, or messages you do nor recognise as they may provide access to hackers.

Online Safety Handbook

Privacy and Identity Theft

What to do if your Identity has been stolen

- Act promptly in order to minimise the impact of the theft.
- Contact any affected websites and advise them about the problem.
- If you can, log in and change your password immediately using a strong password. If you are unable to log in, contact the website's technical support department immediately for further advice. Think about changing your password on other websites in case they have also been compromised.
- If website access requires a secret question, change it if you can, to avoid repeat incidents.
- Ask your bank, building society or credit card company for advice (for example, on freezing accounts and getting new cards, passwords and PINs). Most will refund the full amount lost providing you were not negligent in some way.
- Check your other personal information, such as addresses, to make sure it is still correct.
- Check for other transactions, items for sale or items purchased in your name which you have not originated and cancel them.
- Report all lost or stolen documents such as passports, driving licenses, credit cards, cheque books etc, as soon as possible to the relevant issuing authorities.
- Check with credit reference agencies for any unusual entries, and for advice. For example, Experian, Clear score or Equifax can all offer an inexpensive monitoring service which will notify you if any unusual activity has taken place.
- Notify Royal Mail if you suspect mail theft or that a mail redirection has been fraudulently set up on your address.
- Consider registering with the CIFAS Protective Registration Service.
- For further guidance and support, visit: www.identitytheft.org.uk
- Looking for identity theft resources to share in your community? Visit: https://www.actionfraud.police.uk

Online Safety Handbook

Cyber Bullying

Cyber-bullying, Cyber-harassment or Online Bullying is a form of bullying or harassment using electronic means. Cyber-bullying is when someone bullies or harasses others using the internet and other digital spaces, particularly on social media sites. Harmful bullying behaviour can include posting rumours, threats, sexual remarks, a victims' personal information, or pejorative labels (i.e., hate speech).

Bullying or harassment can be identified by repeated behaviour and an intent to harm. Victims of cyber- bullying may experience lower self-esteem, increased suicidal ideation, and a variety of negative emotional responses including being scared, frustrated, angry, or depressed.

All bullying, whatever the motivation or method is unacceptable and should not be tolerated. It can affect anyone, and we are all
potential targets - whether we are adult, child or the bullying is at school, in the community, at work, online or at home.

Signs of cyberbullying:

- Being called names and it is not fun or friendly.
- Being made to feel frightened or threatened.
- Being forced to do something you did not want to do.
- If you are getting insults to do with special needs, disability, race, religion or sexual orientation.
- Pretending to be you by hacking your social media account.
- Starting fights on purpose because some people like to watch or film them.
- Stalking or keeping track of someone and controlling them.
- Someone who is not who they say they are.

Online Safety Handbook

Cyber Bullying

I am being cyberbullied, what should I do?

- Talk to someone you trust or contact the Safe and Sound team at Babington.
- Block the sender.
- Try not to reply as it can make things worse.
- Keep the evidence or ask someone to help you do this and be sure to say how often this has been happening.
- If it is another learner within your online session or a member of Babington staff speak to the Safeguarding team at Babington.
- If it is someone at work, speak to your line manager or HR department.
- If it is a message with sexual content that upsets you, talk to a trusted person and together you may report it.
- You might prefer to call a helpline like: www.nationalbullyinghelpline.co.uk

Further Guidance and Support:

- You can get further advice and support from the National Bullying Helpline: www.nationalbullyinghelpline.co.uk.
- The National Bullying Helpline website and helpline is run by Volunteers. We are open from 9am to 5pm Monday to Friday. Freephone: 0300 323 0169.

Local Police Force:

- You can report harassment, malicious messaging or distribution of private sexual images without consent online www.met.police.uk or by calling us on 101. They will confirm if an offence has been committed, based on the full facts and your individual situation.
- In order to assist us with our investigation you must not respond to the message as it may encourage the sender and make the situation worse.

Online Safety Handbook

Inappropriate Content

The internet, apps, messenger services etc. provides many ways to share content with a wider audience. Some content may be illegal, inappropriate, offensive or unsuitable for some age groups.

Some people may deliberately search for inappropriate content. You might accidently open content by typing in the wrong web address or clicking on pop-up advertisements or links in emails.

New research commisoned by the Internet watch Foundation shows 14% of young people aged 18-24 report having come into contact with, or stumbling across, websites showing Child Sexual abuse, images or videos. A further 10% of people aged 25-34 also reported they had been exposed to child sexual abuse material online.

Inappropriate or unsafe content might include:

- Pornography.
- Violence.
- Extremist behaviour.
- Sites advocating criminal and anti-social behaviour.
- Offensive content such as text, photos or videos on social media.
- Chatrooms or blogs that encourage racism or hate.

Things you can do to protect yourself:

- Be aware of the potential online risks.
- Check or set up safe search settings, or parental controls on the devices or applications you use.
- You can also opt to activate the safety mode on YouTube, iTunes and Google Play.
- Avoid pop-ups, they can often contain malware or link to inappropriate websites.
- Activate the safety measures or settings offered by different sites. Social networking sites like Facebook, Instagram, Snapchat, TikTok, X (Twitter) all have privacy settings that will help you control who has access to your content and what you or they see.

Online Safety Handbook

Online Reputation

An online reputation, or e-reputation, is the reputation of a company, person, product, service or any other element on the Internet and digital platforms.

The things online that you have liked, shared and commented on, as well as what others have shared about you, may shape what other people think about you; this is your online reputation.

Importance of a good online reputation

As colleges and employers turn to the internet to find out more about potential candidates, what we post online can have a real impact on our lives offline. So, helping our learners to understand the long-lasting effects of what they share and empowering them to take control of how their online reputation is created is key.

Why does my online reputation matter?

Your online reputation could affect how people think about you or even behave towards you. Your online reputation may play a
part in big decisions about your future, for example whether someone will offer you a job you apply for.

What is a digital footprint?

Your digital footprint is the mark that you leave behind when using the internet and can shape your online reputation. Your digital footprint is made up of the content you create post and share; as well as the content that others post, and share, with you and about you.

How do I see my own digital footprint?

The best way to see your digital footprint is to search your name online. Using a search engine, find out what information about you is visible to the public. If you have a common name, you may find it helpful to add other key words, such as the place you live or the name of your college, to the search.

Online Safety Handbook

Online Reputation

How can I remove negative things appearing when people search my name online?

If you have shared something online that you regret (e.g., an embarrassing photo or offensive joke) the best thing to do is delete the original post. If someone else has shared something negative about you, start by removing any tags that link directly to your account and asking the person who posted the content to delete it. If they refuse, there may be options to report it and have it deleted that way. Sometimes you may find that lots of people have shared something, making it difficult to remove completely, in this situation it is important to see help and support.

Will privacy settings protect everything I share online?

Privacy settings are a useful tool to help protect the things you share online, but they are not a guarantee that your content is secure. Your friends or followers can screenshot your content and share it on, or they may show other people using their device.

What should I do before sharing or posting something online?

Take time to think, how will this reflect on you now and in the future? Be careful not to share personal information, content that
might upset or offend others, or content that you may be embarrassed by in the future.

I have posted something online that I regret, what can I do?

Do not panic and take it down as quickly as possible, to limit the possibility of it getting shared on. If you think you might have upset somebody with what you shared, reach out to them, and remember that saying sorry can be powerful! If it does come up in the future, be honest and acknowledge what you have learnt from your mistake.

Tips: Think carefully before posting. Deactivate and delete old accounts which you no longer use to remove out-of-date content from your digital footprint.

Make a positive footprint! The internet is a tool so make good use of it – raise money for charity or do something creative for people to find when they search your name online.

Online Safety Handbook

Online Grooming

Online grooming is a form of abuse that involves manipulating someone until they're isolated, dependent, and more vulnerable to exploitation.

Online grooming can happen on social media, gaming sites, or any site that allows individuals to communicate with one another. Since this kind of grooming happens online, the signs may be harder to recognise.

Try thinking about grooming, specifically online grooming, as a long game. It is a gradual process where the abuser picks their target, build up trust, and the actual abuse, which is usually sexual or financial, doesn't come until much later. It is a process of coercion and manipulation.

Signs of you may be being groomed:

Groomers often lie about who they really are, making it hard to know whether someone is genuine online, signs to look out for include:

- Bombarding you with messages.
- Asking you to keep your conversations secret.
- Trying to find out more about your personal life.
- Sending sexual messages.
- Trying to blackmail you.
- Tapping into your own vulnerabilities

Online Safety Handbook

Online Grooming

Spotting the signs someone is being groomed online

Here are some of the signs of grooming you should look out for:

- The person becomes withdrawn, or they may seem troubled by something but unwilling to talk about it. Alternatively, their emotions might become more volatile.
- You notice them using or wearing something new, that you did not buy for them.
- Groomers often aim to isolate their targets from their family or friends. If they seem reluctant to see you, or they refuse a visit, it might be because someone is manipulating them.
- You notice that sums of money have disappeared from the person's bank account, or the person claims they cannot pay for
food or bills.
- The person might be spending more time on the phone, or online, than usual. But they will not say what sites they're visiting, or who they are talking to.
- They start talking about a new "friend", "boyfriend" or "girlfriend", and it's not clear who they are or how they met them.
- Grooming can also lead to radicalisation. In which case, you might notice that the person starts talking about an issue or a cause that is never really interested them before.

Online Safety Handbook

Online Grooming

Preventing Online Grooming:

Whilst the internet can be a great way to communicate and socialise, we urge you to take care when talking to new people online. Social media and online dating sites can be popular tools for pedophiles and rapists to target individuals by watching what they are doing and building false relationships.

Our top tips for staying safe online is to:

- Remember that once something is sent online it can never be removed.
- Not give out your personal details.
- Trust your instincts. If you think something feels wrong, let us know.
- Not do anything you do not want to do - speak to someone you trust if you are feeling pressured to meet or talk to someone.
- Tell people you trust where you are going if you decide to meet up with someone you have not met before.
- Tell the person you are meeting that people are aware of where you are.

Reporting Online Grooming:

- You can report any online grooming to CEOP by clicking: www.ceop.police.uk/ceop-reporting/
- CEOP is part of the National Crime Agency and help to keep you safe online.
- If you are worried or concerned about something, please make sure you speak to an adult you trust.
- Alternatively, you can call Childline where you can talk anonymously: 0800 1111.
- If you or someone else is in immediate danger, then please call 999.

Online Safety Handbook

Online Pornography

What do I need to know about online pornography?

As younger people explore the internet, they can sometimes come across sexual content accidentally, and some of what they become exposed to may be unpleasant, hardcore pornography and extreme images. But there are steps you can take to limit their exposure to this kind of inappropriate content.

What is the impact on a Younger person seeing porn?

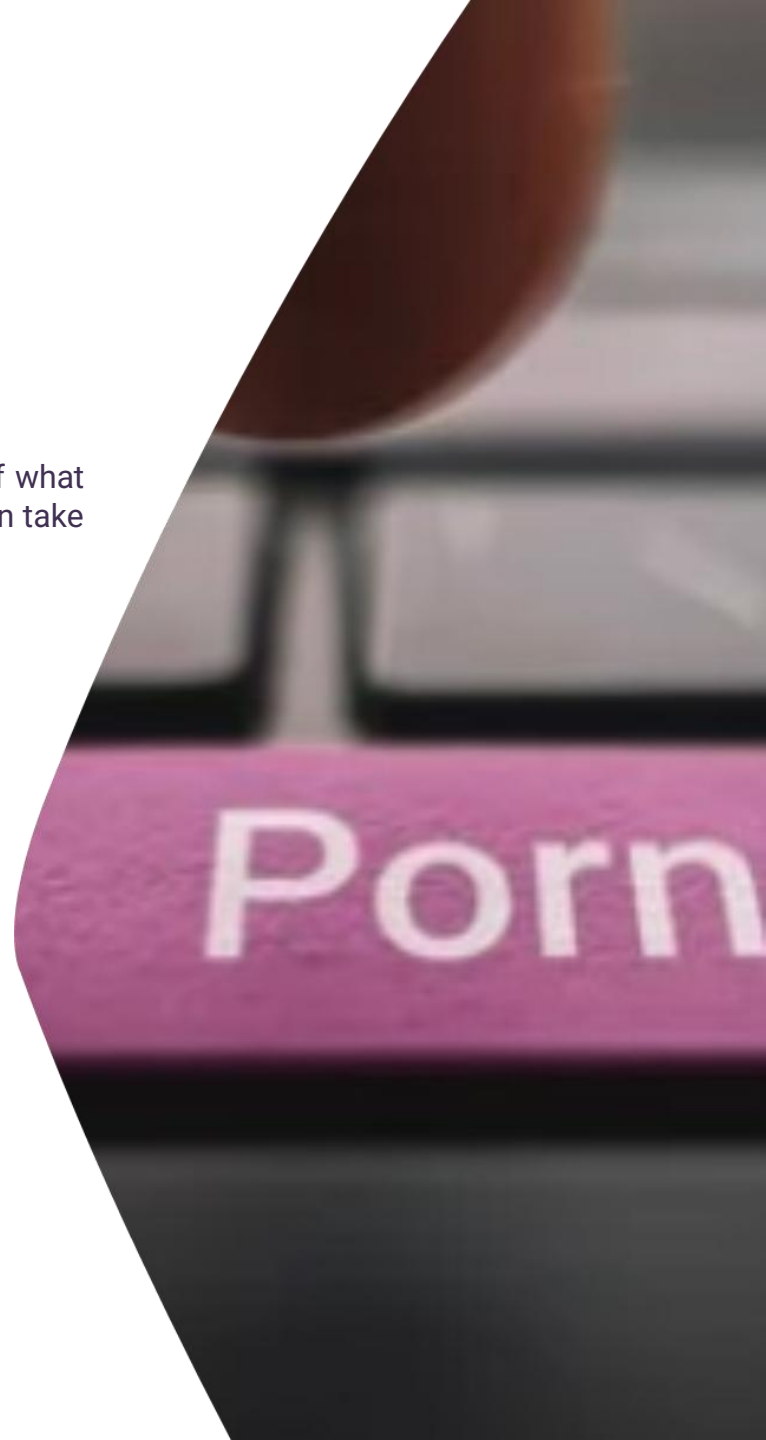
- It may distort their understanding and expectation of sex and relationships.
- They can show signs of early sexualised behaviour and it may affect their sexual identity.
- It can lead to inappropriate expectations of girls and women and treating them more like objects.
- Girls may feel pressure to live up to these unrealistic expectations of sex.
- May develop feelings of anxiety or depression.
- Become obsessed with acting out adult sexual acts they've seen.
- It can also affect their body image and sense of what is normal for a girl or a boy.

What can I do to help block internet pornography?

- Set your search engine to "Safe search" mode.
- Use the family safety tools provided with your device's operating system.
- Disable access to adult sites on workplace and public wifi use appropriate filtering & Monitoring services.
- On mobile phones unsure you use a Safe search engine.

For further information on how to block sites and protect younger people take a look at:

www.internetmatters.org



Online Safety Handbook

Sexting and Revenge Porn

What is Sexting?

Sexting is when people share a sexual message and/or a naked or semi-naked image, video or text message with another person. It's also known as nude image sharing.

Young people may consent to sending a nude image of themselves. They can also be forced or coerced into sharing images by their peers or adults online.

What is revenge porn?

If a relationship ends and an image is shared around peer groups this is revenge porn, it may lead to bullying and isolation, Perpetrators of abuse may circulate a nude image more widely and use this to blackmail a child and/or groom them for further sexual abuse.

It's a criminal offence to create or share explicit images of a child / Young person, even if the person sharing is a minor themselves. If sexting is reported to the police, they will make a record but may decide not to take any formal action against a young person.

In all instances report this to the Police immediately.

Remember there are support service out there to help and get images removed from the internet: www.ceop.police.uk/Safety-Centre/

Online Safety Handbook

Radicalisation

What is Radicalisation?

Radicalisation is the process through which a person comes to support or be involved in extremist ideologies. It can result in a person becoming drawn into terrorism and is in itself a form of harm.

So how can I become radicalised online?

We don’t go online we live online! For most of the day each person is connected to the internet in some way or another. Maybe your role is working online in an office, working remotely at home, or just using your mobile phone / smart watch as all have internet access. The internet therefore has opened up many new ways of communicating with others through the use of chatrooms, online multiuser games, social media platforms giving way for extremists the means to target, connect and communicate with people who may be vulnerable to radicalisation.

- It's about "Push and Pull factors" Anyone can be at risk of being radicalised regardless of their age, but teenagers and young people can sometimes be at a greater risk. This is because they might be entering a new phase in their lives, such as going to college or university. Or they might be struggling with a sense of identity or belonging.
- Extremists know how to capitalise on feelings of insecurity and convince the person they can help by providing a solution.
- They don’t have the person’s best interests at heart and will twist the narrative to suit their end goal of radicalisation.

Radicalisers use social media to identify vulnerability.

- Social media platforms and internet forums are full of people reaching out online to combat feelings of isolation and loneliness, stress, anxiety or rejection. This can sometimes leave them feeling very upset or angry and potentially at risk from people looking to exploit these feelings. A radicaliser will try to connect with them or will join in the forum chat posing as a ‘listening ear’ or a ‘friend.’

Exposure to extremist content and groups online can lead them down a dangerous path. If you're concerned someone you know might be targeted, then act early and share your concerns with **Safeguarding@babington.co.uk**

Online Safety Handbook

Digital or Cyber Self-Harm

Why do people cyber self-harm?

To get a better understanding of why people do this, Psychotherapist and Counselling Directory member, Simon Mathias who has worked with teenagers who have cyber self-harmed says, in his experience, there are three main reasons why they do this: To get attention, For social compatibility, To receive positive remarks. The attention-seeking reason may appear controversial. In the self-harm community, the misconception that it is attention-seeking is fiercely refuted. This is where cyber self-harm differs. Those who engage in it often want others to notice.

"They see others being supported when they report trolling. This is then endorsed by the reactions of the media when celebrities report incidents. They tend to want to have attention paid to them by friends, peers, or teachers, rather than by parents."

Social compatibility is often the reason when the cyber self-harm activity results in being accepted or liked by others, and the desire for positive remarks can go deeper than simply wanting attention.

"This is where the person wants specific and direct positive comments, on aspects such as their physical appearance, what they have done etc. It may be directed to get a response from parents or family, but most certainly friends, and usually to counter the specific trolling comments."

What are the risk factors for digital self-harm?

- Researchers suggest that a range of underlying factors such as family issues, physical illness, or psychological aspects, might explain digital self-harm behaviour.
- The use of drugs or alcohol.
- Sexual orientation (those who identified as gay, lesbian, or bisexual were three times more likely to report the behaviour).
- Previous experience with school bullying (four to five times more likely to report the behaviour).
- Previous experience with cyber bullying (seven to twelve times more likely).
- Deviant behaviour (7% in the survey who had digitally self-harmed had also engaged in physical self-harm.

Online Safety Handbook

Digital or Cyber Self-Harm

Identify digital self-harm

While it is important to recognise that this type of self-abuse can occur, the incidence of digital self-harming behaviour amongst adolescents remains very low worldwide. If this behaviour does occur, it may well co-exist with other online and offline factors. Reasons for digital self-harm vary, however, motivations fall into two 4 broad categories: looking for attention and/or support.

There are several approaches which parents, carers and/or professionals can take to help to identify whether their adolescent(s) is engaging in digital self-harming behaviours:

Create an open and trusting environment: Adolescents can be helped to open up if they are experiencing feelings of low self- worth by creating open and trusting environments. Establish and maintain safe relationships so that young people feel that they are able to go to parents/ carers or professionals about self-trolling. Be prepared to be realistic, trust will take time to achieve.

Social media and online use: Be prepared to have ongoing conversations with young people about their use of social media and other online platforms. Enquire about any negatively charged comments, giving the young person opportunity to share their feelings about them. Parents can remain vigilant for signs of self-harm online. Parents can help their children get a perspective around cyberbullying and what to do if it happens to them.

Avoid making judgements: Making judgements should be avoided. Instead, try to ask open ended questions which will help adolescents work through incidents of digital self-harm. Example questions might include, “How did you feel as you were posting these messages?” “How did others respond?” “What was your reaction to others’ responses?” “How did you feel after it all happened?”

Help build a support system: Help with the creation of a list of trusted individuals such as teachers, trusted friends, counsellors or others who can help to support the individual. Building trust & a willingness for the young person to reach out might take time.

Seek professional support: Young people who display digital self-harming behaviours might well benefit from accessing professional support from a specialist mental health practitioner to address the underlying issues and to learn appropriate coping strategies.

Online Safety Handbook

Filtering & Monitoring

Filtering and monitoring are essential strategies for managing digital environments both at home and in the workplace. They help in protecting against harmful content, maintaining security, and ensuring productivity. Below is a concise guide on implementing filtering and monitoring effectively:

1. Define Your Goals

- **Security:** Protect against malware, phishing, and other cyber threats.
- **Content Control:** Restrict access to inappropriate or non-work-related content.
- **Productivity:** Ensure time is spent on relevant tasks.
- **Compliance:** Meet legal and regulatory requirements, particularly in sensitive industries.

2. Choose the Right Tools

- **Web Filtering:**
  - **For Home:** Use parental control software like **Net Nanny** or **Qustodio** to block inappropriate content and manage screen time.
  - **For Work:** Implement enterprise-level web filtering solutions like **Cisco Umbrella** or **Barracuda Web Security** to block access to non-essential websites and secure the network.

•**Email Filtering:**
  - Deploy email filtering solutions like **Proofpoint** or **SpamTitan** to filter out spam, phishing attempts, and malicious attachments.

•**App and Device Monitoring:**
  - **For Home:** Tools like **Google Family Link** or **Microsoft Family Safety** allow monitoring of app usage and setting restrictions on children's devices.
  - **For Work:** Software like **Teramind** or **Hubstaff** provides detailed monitoring of employee activity, including time tracking, app usage, and keystrokes.

Online Safety Handbook

Filtering & Monitoring

3. Implement at the Right Level

- **Device-Level Filtering:** Install software directly on individual devices for more granular control. Ideal for personal computers and mobile devices.
- **Network-Level Filtering:** Apply filters at the router or firewall level to control access across all connected devices, useful for both home networks and corporate environments.

4. Set Clear Policies

- **Home:** Define rules for screen time, acceptable content, and online behaviour. Discuss these openly with family members, especially children, to foster understanding and cooperation.
- **Work:** Create a clear acceptable use policy (AUP) that outlines what is permissible during work hours. Communicate this policy clearly to all employees and ensure they understand the purpose behind monitoring and filtering.

5. Monitor Effectively and Respectfully

- **Regular Reports:** Set up automated reports on internet usage, app activity, and email filtering to stay informed without constant manual checks.
- **Privacy Considerations:** Balance the need for monitoring with respect for privacy, particularly in the workplace. Ensure that monitoring is focused on security and productivity, not invasive surveillance.

Online Safety Handbook

Filtering & Monitoring

6. Adjust and Update Regularly

- **Adapt to Changes:** Regularly review filtering and monitoring settings to adapt to changing needs, whether that's a child growing older or evolving cybersecurity threats at work.
- **Update Software:** Keep all filtering and monitoring software up to date to protect against the latest vulnerabilities and threats.

7. Provide Education and Training

- **Home:** Educate family members about the dangers of the internet and the reasons behind certain restrictions.
- **Work:** Offer training sessions on cybersecurity best practices, safe browsing habits, and the importance of adhering to company policies.

8. Evaluate and Optimize

- **Review Effectiveness:** Periodically assess whether the current filtering and monitoring setup is meeting your goals. Look for areas of improvement and adjust settings or tools as needed.
- **Seek Feedback:** In a workplace, gather feedback from employees about the impact of monitoring on their work and address any concerns.

By following these steps, you can implement effective filtering and monitoring strategies that protect and enhance the digital environment, whether at home or in the workplace.

Online Safety Handbook

Artificial Intelligence. (AI)

Keeping yourself safe while interacting with AI online involves understanding how to use AI responsibly, protecting your personal information, and being aware of the potential risks. Here's a guide to help you navigate AI safely:

1. Be Aware of Privacy and Data Security

- **Limit Sharing Personal Information:** Avoid sharing sensitive personal information with AI tools, especially those online. This includes your full name, address, phone number, financial information, or anything that could be used to identify you.
- **Use Strong Passwords:** Protect your accounts on platforms using AI with strong, unique passwords, and enable two-factor authentication where possible.

2. Understand AI Limitations

- **Recognise AI's Limitations:** AI systems may not always provide accurate or complete information. They can make mistakes, so always verify critical information through reliable sources.
- **Avoid Over-Reliance:** Don't rely solely on AI for decisions involving your health, legal matters, or finances. Consult professionals for these areas.

Online Safety Handbook

Artificial Intelligence. (AI)

3. Stay Informed About AI Developments

- **Educate Yourself:** Keep up with the latest news and developments in AI. Understanding how AI works can help you use it more effectively and safely.
- **Beware of Biases:** AI systems can reflect the biases present in their training data. Be cautious of biased recommendations or outputs.

4. Use Trusted Platforms

- **Stick to Reputable Services:** Use AI tools from well-known and trusted platforms. Be cautious of new or unknown services that might not have strong security practices.
- **Check Reviews and Ratings:** Before using any AI-powered tool, check user reviews and ratings to gauge its reliability and safety.

5. Be Cautious of Scams and Malicious AI

- **Watch for Scams:** Scammers may use AI to create convincing phishing emails, fake profiles, or deepfake content. Be sceptical of unsolicited communications and offers that seem too good to be true.
- **Report Suspicious Activity:** If you encounter a suspicious AI tool or interaction, report it to the platform and avoid engaging further.

Online Safety Handbook

Artificial Intelligence. (AI)

6. Maintain Ethical Use

- **Use AI Responsibly:** Ensure your use of AI aligns with ethical standards. Avoid using AI to deceive, manipulate, or harm others.
- **Respect Privacy:** When using AI that involves others, such as chatbots or recommendation systems, respect their privacy and data rights.

7. Protect Mental Well-being

- **Limit AI Interaction:** Spending too much time interacting with AI can affect your mental health. Set limits on your usage to avoid over-dependence.
- **Use AI for Positive Outcomes:** Focus on using AI tools that enhance your productivity, learning, or well-being rather than those that could lead to negative emotional impacts.

8. Review AI-generated Content Carefully

- **Critically Assess AI Content:** AI can generate content, but it's essential to critically evaluate it for accuracy, relevance, and appropriateness before using or sharing it.
- **Avoid Misinformation:** Be cautious of AI-generated misinformation. Verify the authenticity of content, especially if it seems unusual or provocative.

By following these steps, you can enjoy the benefits of AI while minimising potential risks and maintaining control over your online presence.

Online Safety Handbook

Online Safety Act (2025 update)

Key Updates to the UK Online Safety Act 2025

1. Age Verification and Adult Content
- Platforms hosting adult content, including pornography, must verify users' ages before granting access.
- Acceptable methods include photo ID checks, facial age estimation, credit cards, or verified digital identity systems.
- Major adult sites in the UK have seen substantial declines in traffic following the implementation of these measures.

2. Protection of Children
- Platforms must prevent children from accessing harmful material, including content that encourages self-harm, suicide, or eating disorders.
- Age assurance is now mandatory to ensure under-18 users cannot access adult content.
- Platforms are also required to provide accessible reporting tools and filters to reduce exposure to harmful content.

3. Regulatory Enforcement
- Ofcom, the UK communications regulator, can enforce compliance, impose fines, or block platforms that fail to meet the rules.
- Legal challenges, such as Wikipedia's case, have clarified that even educational or information platforms can be subject to certain obligations if they are considered high-risk or widely used.

4. Unintended Consequences and Criticism
- Some users have started using VPNs to bypass age verification restrictions.
- Critics argue the rules may impact privacy and freedom of expression, with smaller or educational platforms facing compliance challenges.

5. Overall Impact
- The Act strengthens protections for children and imposes stricter duties on platforms hosting user-generated content.
- However, it also raises practical challenges for implementation and ongoing concerns about online freedoms and privacy.

Online Safety Handbook

Summary of Support

- **If you have any questions regarding this Online Safety Handbook, please email: safeandsound@babington.co.uk**
- **Should you need any support, advice or guidance or have a concerns, please contact: safeguarding@babington.co.uk or call: 07557 265040**
- **The Babington Safe and Sound Team are available Monday to Friday between 8:30 and 17:00.**

If you require urgent support outside of these hours, please contact your GP, Out Of Hours Service, NHS 111, or in case of emergency visit you're A&E Department or call 999.

Helpful Website Links:

- **Identity Theft:** www.identitytheft.org.uk
- **Online Cyber Bullying:** www.nationalbullyinghelpline.co.uk
- **CEOP National Crime Agency:** www.ceop.police.uk
- **Internet Matters Online Safety:** www.internetmatters.org
- **Cyber Smile Foundation:** www.cybersmile.org
- **NSPCC**: www.nspcc.org.uk
- **Support for Parents and Carers:** Keep Children Safe Online - GOV.UK (www.gov.uk)
- **UK Safer Internet:** www.saferinternet.org.uk
- **Police:** Call 101, or 999 in the event of an emergency or visit www.police.uk