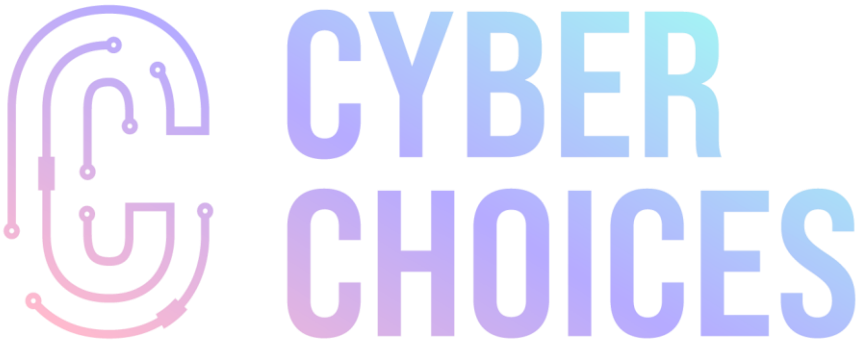
Derby and Derbyshire

Cyber Choices Toolkit



February 2023
Version 1.7

PUBLIC

Author

Document produced by Derbyshire County Council, Community Safety Unit, on behalf of, and in consultation with:-

- Derbyshire Constabulary, local Cybercrime Unit
- East Midlands Special Operations Unit (EMSOU), regional Cybercrime Unit
- Derby and Derbyshire Safeguarding Children Partnership
- Derby City Safeguarding Adults Board
- Derbyshire Safeguarding Adults Board
- Derbyshire County Council, Legal Services
- National Police Chief's Council (national Cyber Choices lead)

Change History

Date	Version	Reason
8/6/20 – 20/8/20	Versions 0.0 – 0.4	Development drafts
27/8/20	Version 1.0	Approved by Derby and Derbyshire Safeguarding Children Partnership Policy and Procedures Sub-Group, subject to further consideration of information sharing.
3/9/20	Version 1.0	Approved by Derbyshire Safer Communities Core Group, subject to resolution of issues raised by Derby and Derbyshire Safeguarding Children Partnership Policy and Procedures Sub-Group
24/9/20	Version 1.0	Approved by Derbyshire Safer Communities Board, subject to resolution of issues raised by Derby and Derbyshire Safeguarding Children Partnership Policy and Procedures Sub-Group
20/5/21	Version 1.1	Revised to incorporate revised referral process, recommendations from Derbyshire Constabulary legal department re information sharing and findings of the latest NCA Intelligence Assessment Report.
10/2/22	Version 1.2	Revised to incorporate revised referral process, new logo and changes identified by DPIA.
21/6/22	Version 1.3	Toolkit reviewed for accuracy of links
5/7/22	Version 1.4	Approved by Derbyshire County Council Information Governance Group, subject to resolution of recommendations from the DPIA.
14/7/22	Version 1.4	Approved by Derby and Derbyshire Safeguarding Adults Board Policy and Procedures Sub-Group, subject to some terminology changes in relation to vulnerable adults and resolution of recommendations from the DPIA.
4/8/22	Version 1.5	Approved by Derby and Derbyshire Safeguarding Children Partnership Policy and Procedures Sub-Group, subject to clarification of consent requirements and resolution of recommendations from the DPIA.
26/10/22	Version 1.6	Revised to reflect National Police Chief's Council (NPCC) approach to information sharing for Cyber Choices, under safeguarding legislation, and DPIA recommendations.
3/11/22	Version 1.6	Approved by Derby and Derbyshire Safeguarding Children Partnership Policy and Procedures Sub-Group.
10/11/22	Version 1.6	Approved by Derby and Derbyshire Safeguarding Adults Board Policy and Procedures Sub-Group.
10/11/22	Version 1.6	Approved by Derby and Derbyshire Online Harms Sub-Group.
1/12/22	Version 1.6	Approved by Derbyshire Safer Communities Board.
17/2/23	Version 1.7	Additional resources included in 'Useful Websites'

Contents

INTRODUCTION

Cybercrime now accounts for almost 50% of crime in the UK. It is increasingly easy to commit cybercrime, with hacking tools and guides readily available online.

Research suggests that 61% of hackers began hacking before the age 16[1] but some may be as young as 10[2], with estimates showing that 1 in 4 teenagers have tried some form of cybercrime[3] (many without realising it).

There is a real need to intervene early, before young people ever become involved in cybercrime, so that their technical skills can be harnessed. Skills in coding, gaming, computer programming and cyber security are in high demand, meaning there are excellent career opportunities for anyone with an interest in IT.

The Cyber Choices toolkit is aimed at professionals working with young people and vulnerable adults, who they are concerned about because:-

- they have a high technical ability in computing and are vulnerable, or at risk of cyber exploitation;

  or

- they are already on the cusp of cyber criminality.

This toolkit will help you:-

- Identify individuals who are at risk of becoming involved in cyber-dependent crime.
- Refer those who would benefit from a Cyber Choices intervention.
- Appreciate how a multi-agency approach can deter young people, and vulnerable adults, from cyber-dependent crime.
- Understand your role in preventing cybercrime and securing a positive outcome for more young people and vulnerable adults.
- Appreciate the importance of educating parent(s)/guardian(s)/carer(s) in online safety.

This toolkit should be read in conjunction with existing safeguarding policies and procedures, including:-

- Your own agency's safeguarding children and safeguarding adult policy and procedures.
- Derby and Derbyshire Safeguarding Children Partnership multi-agency procedures, in particular the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment.
- Derbyshire and Derby City Safeguarding Adult Boards joint policy and procedures

[1] National Crime Agency Intelligence Assessment 'Pathways into Cyber Crime' 2017

[2] National Crime Agency Intelligence Assessment 'Pathways in Cyber Crime in the UK' 2021

[3] Youth Pathways into Cybercrime

What is cybercrime?

Cybercrime is an umbrella term for crimes where technology is a means, and/or a target, for the attack, or those crimes which take place online. As our use of technology increases, cybercrime is becoming a growing problem, targeting individuals, companies and government organisations. Cybercrime can be split into two broad categories:-

Cyber-dependent crime – These are offences, under the Computer Misuse Act 1990 (See APPENDIX A – COMPUTER MISUSE ACT 1990), which can only be committed using a computer, a device, computer network or other form of information communications technology (ICT).

Examples of *cyber-dependent* crime include:-

- 'Hacking', which involves gaining access to someone's computer network, without their permission, and then taking control and/or taking information.
- Making, supplying or obtaining malware, viruses, spyware, ransomware, botnets or remote access trojans to get into other people's computers.
- Carrying out a DDoS (Distributed Denial of Service) attack to overwhelm, or 'crash', a website or 'booting' someone offline, whilst playing online games.

Cyber-enabled crime – These are offences that can be conducted on or offline but, when online, it may take place at unprecedented scale and speed.

Examples of *cyber-enabled* crime include bullying, fraud, grooming, identity theft, sexual abuse, sexual exploitation, stalking.

To help understand cyber terminology, a glossary is available at https://www.saferderbyshire.gov.uk/what-we-do/cyber-crime/cyber-crime.aspx

Criminal exploitation

Some cybercrimes are committed by individuals, others by organised crime groups, who are experts at 'grooming' vulnerable, technically skilled individuals to launder their money or launch their cyberattacks. There are also examples of young people being groomed to use the 'dark web' to purchase guns and drugs for gangs or organised crime groups.

This is known as criminal exploitation, which occurs where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child under the age of 18, or a vulnerable adult. The victim may have been criminally exploited even if the activity appears consensual. Criminal exploitation does not always involve physical contact; it can also occur through the use of technology.

There are few known examples of this type of exploitation and it is considered unlikely[2] that criminal exploitation is a major pathway into cybercrime.

When referring to cybercrime, this toolkit only relates to cyber-dependent crime - for concerns about any form of online abuse, you should follow existing safeguarding procedures.

[2] National Crime Agency Intelligence Assessment 'Pathways in Cyber Crime in the UK' 2021

INDIVIDUALS AT RISK OF BEING INVOLVED IN CYBERCRIME

Why do people become involved in cybercrime?

In 2017, the National Cyber Crime Unit found that the average age of a cybercriminal, when arrested, was 17, which is significantly lower than that of those involved in traditional types of crime, such as burglary[1]. However, the latest intelligence suggests that the average age of initial cyber offending may have fallen to 15. This may be linked to the increase in children involved in online gaming[2].

Research suggests that teenagers (overwhelmingly male), who are unlikely to be involved in traditional offline crime, are becoming involved in cybercrime. 61% of hackers began before the age of 16[4].

The National Crime Agency have undertaken 'debriefs' with former cyber criminals to help us understand why and how people become involved in cybercrime[1]. They found that people were motivated to become involved in cybercrime because:-

- They have a deep **interest in technology**.
- They have a desire to **prove themselves** and **improve** their technical skills.
- They focus on **negative role models**, who are often the cyber criminals at the top of the ladder they are trying to climb.
- They get satisfaction out of **solving** difficult **problems** and completing a **challenge**.
- They are addicted to 'getting to the next level' (within games) and the **notoriety** this gives.
- Hacking offers them a way of acquiring **power** over others (their victims).
- Membership of 'hacking forums' gives them a '**sense of belonging**' from their peers.
- They gain **recognition, status** and a **reputation** in the 'hacking world'.
- It is '**fun**'.
- It furthers their '**political ends**'.
- There is potential for **financial gain** (although this is often a secondary motivation).

[1] National Crime Agency Intelligence Assessment 'Pathways into Cyber Crime' 2017

[2] National Crime Agency Intelligence Assessment 'Pathways in Cyber Crime in the UK' 2021

[4] UNICRI Hackers Profiling Project 2012

There are a number of reasons why people are not deterred from getting involved in cybercrime, such as:-

- They **do not understand** the Computer Misuse Act, so don't realise they are committing a crime.
- They **don't realise the consequences** of their actions, either for themselves or their victims.
- Being online makes them feel **anonymous**.
- The **lack of visible enforcement** presence online.
- The **perception** that cybercrime is **not a priority** for law enforcement agencies and their 'low-level' crimes are **not serious enough** to attract attention.
- Being **unaware of the opportunities** to use their cyber skills legitimately.
- Their **parents and other responsible adults**, such as teachers, Children's or Adult Services, **do not understand** what they are getting involved in, due to their own lack of technical knowledge.
- The **perception** that it is a **victimless crime**.

It must be remembered that only a small number of 'low-level' cyber criminals will go on to reach the higher level of the very technically skilled cyber criminal[1].

How do people become involved in cybercrime?

Often people become involved in cybercrime without realising they are committing a crime or considering the consequences of their actions.

People become involved in cybercrime through:-

- **Online gaming culture**, where it is considered normal to use 'booting' tools to force other users offline during a game.
- **Step-by-step tutorials** and **'off the shelf' hacking tools**, which are advertised openly on low-level hacking or gaming forums. They require limited technical expertise to use and are available at little, or no, cost to the user. Video guides, and step-by-step tutorials, on how to use these products, are also readily available on the open web and social media platforms that are popular with young people such as YouTube, Snapchat, Instagram, TikTok and Twitch.
- Participation in **gaming cheat websites** and '**modding'** (game modification) **forums** and then progressing to criminal **hacking forums**.
- Membership of online coding or hacking forums may lead to them **being groomed** by individuals or groups involved in cybercrime, who encourage them to participate in illegal online activities.

The latest NCA research[2] shows that online gaming is the main pathway into low-level cyber offences, and to a lesser extent, social media account takeovers. The individual has often been a victim of cybercrime themselves and this prompts them to experiment with hacking tools to take revenge.

The progression towards cybercrime is illustrated in Figure 1. It is important to identify and engage with individuals, who might follow this pathway, at the earliest opportunity.

[1] National Crime Agency Intelligence Assessment 'Pathways into Cyber Crime' 2017

[2] National Crime Agency Intelligence Assessment 'Pathways in Cyber Crime in the UK' 2021

Figure 1 – Pathways to illegal online activity [5]

<u>Individual characteristics of a cybercriminal</u>

Further research is being undertaken but, from the limited research that is currently available, Middlesex University[6] identified the following characteristics of young people involved in cybercrime:-

- Adolescent
- High IQ
- Highly computer literate and highly curious about technology
- Broad range of social classes
- Often male
- Socially isolated, but commonly networked with a group of similar adolescents
- Socially awkward and withdrawn, with some 'vulnerability'
- High need for online affiliation and affirmation.

The NCA assessed[2] the most reliable indicators of those individuals likely to commit cyber offences to be:-

- High IQ
- Interest in technology
- Socially isolated
- High appetite for engaging in risky behaviour.

For these characteristics to lead to cyber criminality, there must also be additional factors, such as being a victim of cybercrime or being involved with a group already committing cybercrime.

---

[2] National Crime Agency Intelligence Assessment 'Pathways in Cyber Crime in the UK' 2021

[5] CREST report – Identify, Intervene, Inspire

[6] Youth Pathways into Cybercrime 2016

Indicators of a significant interest in computing or cyber security

Below are some indicators (in no particular order) of an individual's significant interest in computing or cyber security. These indicators, combined with additional vulnerabilities, **may** increase the likelihood of them being vulnerable to their cyber skills being exploited by cyber criminals.

- Deep interest and/or understanding of how communications and computing technology work. This might include phones, tablets, laptops, PCs, games consoles, TV, the internet.
- Curiosity about how technologies interact with each other and what 'vulnerabilities' they have.
- Good knowledge of computer coding.
- Experimenting with tools and techniques discovered online (e.g. YouTube or discussion forums).
- Academically gifted, particularly in terms of technology, but not adequately challenged at school.
- Spending increasing amounts of time, in their bedroom, online and immersed in computing technology.
- They tell a friend, parent or teacher about their newly gained IT skills.
- They have multiple social media profiles on one platform.
- They have multiple email addresses.
- They spend most of their free time alone with their computer.
- They have few 'real friends', but talk extensively to online friends about computers.
- A keen interest in computers, almost to the exclusion of all other school subjects.
- They're online so much it affects their sleeping habits.
- Monitoring tools you've put on the computer might suddenly stop working.

Indicators of involvement in cybercrime

There is no single indicator of an individual's involvement in cybercrime, but the following examples will help you identify whether a young person, or a vulnerable adult, is involved in cybercrime.

- They brag about their hacking skills or knocking someone out of a game.
- They know confidential information, which could only have been obtained by reading a parent's or teacher's email.
- 'Shoulder surfing' to observe passwords.
- Higher than normal levels of secrecy in terms of technology e.g. use of encryption tools, clearing browser history and log files.
- Extreme anxiety about being hacked.
- Use of hacking terminology, such as pwnd sites, DDoS, doxing, 'modding', dossing, bots, botnets, cracking, hash (a type of encryption rather than cannabis), keylogger, phishing, spoof or spoofing.
- Notifications of hacking from your internet service provider.
- They refer to themselves and their friends as 'hackers' or 'script kiddies'.

- Their computer has a web browser called Tor (The Onion Router), which is used to access hacking forums on the dark web.
- They can bypass school and parental controls.
- They can connect to the WiFi of nearby houses (especially concerning if they have no legitimate reason to have the password).
- They claim to be making money from online computer games (many hackers get started by trying to break computer games in order to exploit flaws in the game and then sell these 'cheats' online).
- Your internet connection regularly slows, or goes off, and there is no known reason for this.
- Regular deliveries of unknown packages.
- Making and taking phone, or VOIP, calls during the night.
- Hacking the school website or systems.

Autism and cybercrime

People with autism often have advanced digital skills. While there is still more to be understood around individuals with autism and their skills and motivations to commit cybercrime, people with autism, and other neurodiversity conditions, can show an exceptional talent for problem solving and pattern spotting, which would be beneficial for careers within the cyber security industry, but this could also put them at risk of becoming involved in cybercrime.

Consequences of being involved in cybercrime

Cybercrime is a serious offence under the Computer Misuse Act 1990 (see APPENDIX A – COMPUTER MISUSE ACT 1990) and all UK law enforcement agencies and international partners will deal with cyber offenders in a robust and dynamic manner.

Individuals getting involved in cybercrime could face:-

- A visit and warning from Derbyshire Constabulary or the National Crime Agency (NCA).
- A Cease and Desist Notice from Derbyshire Constabulary or the National Crime Agency. This is a warning that failure to stop the behaviour will lead to further law enforcement action and would also be used in any future prosecution, as evidence of non-compliance.
- All computer devices and digital storage being seized for investigation.
- Being arrested and kept in a cell overnight, awaiting interview.
- A conviction under the Computer Misuse Act (1990), which could result in:-
  - A caution – with or without conditions
  - A fixed penalty or (unlimited) fine
  - A Serious Crime Prevention Order or Criminal Behaviour Order, which will impose prohibitions, which could include being prevented from using the internet, having police monitoring software on devices and co-operating with the Police Cyber Choices team
  - A prison sentence – the maximum being life imprisonment for the most serious offences.

The consequences of being arrested, or having a criminal conviction, can have an impact on their long-term future, including:-

- **Education**
  - Some courses may not permit entry.
  - School, college or university places may be withdrawn.
- **Employment**
  - Future career opportunities will be limited.
  - Under the Rehabilitation of Offenders Act, a conviction has to be declared for a set period of time.
  - Some companies will not employ anyone with a criminal conviction.
  - Convictions may be publicly reported, and many employers will search online records, as part of their recruitment process.
- **Overseas travel restrictions**
  - Visas for entering countries, such as the USA and Australia, will not be granted.
- **Obtaining credit**
  - Credit applications (e.g. student loans, credit cards) may be declined.
- **Insurance**
  - Some car and home insurance companies deny policies for people with criminal convictions, whilst others will impose higher premiums.
- **Housing**
  - Most mortgage providers require disclosure of criminal convictions.
  - A conviction could result in eviction from a rental property.

Spotting the signs of someone who is involved, or at risk of getting involved, in cybercrime and taking early, positive action, by referring to Cyber Choices, reduces the likelihood of these negative consequences and gives us the opportunity to divert them onto a more positive path, where they can develop their cyber skills and significantly increase their career prospects.

MAKING A REFERRAL TO CYBER CHOICES

What is Cyber Choices?

Cyber Choices is a national initiative co-ordinated by the National Crime Agency and delivered by the Cyber Choices teams, based in the regional Cybercrime Unit, at East Midlands Special Operations Unit (EMSOU) and the local Cybercrime Unit, at Derbyshire Constabulary.

The Cyber Choices network is looking to engage with anyone that you are concerned about because:

- They have a high technical ability in computing, and are vulnerable *or* at risk of cyber exploitation

  or

- They are already on the cusp of cyber criminality.

The aims of the programme are to:-

- Deter individuals from becoming involved in cybercrime in the first instance.
- Prevent individuals from becoming more involved in cybercrime.
- Prevent cyber criminals from re-offending.
- Provide education on the Computer Misuse Act 1990 and the possible consequences of breaking the law.
- Encourage individuals to make informed choices about their use of technology.
- Promote legal and ethical cyber opportunities.

The early intervention programme provides positive role models and mentors to give them a better chance of changing their behaviour and help them to make informed choices that will use their skills in a legal way, resulting in positive career pathways.

Cyber Choices can also be used as a Community Resolution outcome for Computer Misuse Act offences.

Who can make a referral to Cyber Choices?

Anyone who has **concerns** about an individual getting involved in cybercrime can make a referral to Cyber Choices - for example parents, teachers, youth workers, social workers, police officers, youth offending officers, etc.

When to make a referral to Cyber Choices?

You should establish the level of seriousness and harm caused or the potential for harm to be caused, so consider:-

- What has happened?
- Who is involved?
- Is this part of a pattern of behaviour?
- Have parents or other partners noticed similar issues?
- Are there any aggravating factors?
    - Did this incident cause any disruption to the school? eg. loss of access/disruption to school website, online learning platforms or school communication networks?
    - Did the school suffer a loss of data or corruption of files?
    - Did the school suffer loss of teaching time, resulting in an impact on other students?
    - Is there a hate element?
    - Have they expressed any ideological motivation or reason for their actions?
    - Is there evidence of escalating behaviour? Or previous incidents of a similar nature?
    - Is the behaviour related to gang activity or an Organised Crime Group?
    - Does the individual have any additional relevant vulnerabilities, such as:-
        - neurodiversity
        - mental health concerns
        - socially isolated

- living in a chaotic or dysfunctional household, or one in which their skills are not likely to be fostered at home
- in a household with inappropriate ideological influences or gang or organised crime group associations.

The National Police Chiefs Council (NPCC) have produced guidance for schools and their cybercrime flowchart is included at APPENDIX C – CYBERCRIME DECISION MAKING FOR SCHOOLS (NPCC)

There are two important questions:-

- Does the individual meet the criteria for a referral to Cyber Choices?
- Are there any safeguarding concerns? If YES, you must also follow local safeguarding procedures

All concerns, discussions and decisions made, and the reasons for those decisions, should be recorded in writing.

When not to make a referral to Cyber Choices?

Cyber-enabled Crime

If you have concerns about **cyber-enabled crime**, such as youth produced sexual imagery (sexting), cyberbullying, online exploitation, online radicalisation, in relation to a child, you must follow the Derby and Derbyshire multi-agency safeguarding children procedures and, where appropriate, make a referral to Children's Social Care.

If you have safeguarding concerns in relation to an adult, who has care and support needs, you must follow the Derby and Derbyshire Safeguarding Adults policy and Procedures and make a safeguarding adult referral to the relevant local authority. For assistance with making a decision as to whether a case should be a safeguarding adult referral, the Decision Making Guidance can be used as a tool.

Criminal Exploitation

If your concerns relate to the criminal exploitation of vulnerable individuals for their enhanced cyber skills (e.g. to launder the criminal's money or launch their cyberattacks), you must refer to the Children at Risk of Exploitation procedure. A CRE Risk Assessment should be completed, to identify the level of risk, and a referral made to Children's Social Care, as appropriate.

If a child, young person or vulnerable adult is in immediate danger, call the Police immediately on 999.

Cyber Choices Referral Process

The initial steps **the referrer** should make are as follows:-

1. *Talk to the individual*
    - Try and ascertain what they are/have been doing in terms of potential cybercrime and who else they have been getting involved with.
    - Explain the decision to refer to Cyber Choices and how it can help and support them.

2. *Talk to their parent(s)/guardian(s)/carer(s)*
    - Explain the decision to refer to Cyber Choices and how it can help and support them and their child to help prevent/divert them from getting involved in cybercrime.
    - Advise them that details of the referral will be recorded on police systems, for the purposes of delivering the Cyber Choices early intervention programme. (Information would only be shared with other partners with their consent, unless the police identified any new/additional safeguarding concerns, which would be dealt with in accordance with existing safeguarding procedures.) Full information is available on the Privacy Notice.
    - Signpost them to information about Cyber Choices on the NCA website.

3. *Complete the Cyber Choices Referral Form*
    - Email EMSOU at Cyberchoices@leics.police.uk to request the Cyber Choices referral form.
    - Complete the referral form, detailing the reason for the referral. You will need to provide information about the individual's technical ability, together with any insight about what they may intend to do, or are capable of doing, with their skills. Give as much information about your concerns as possible, but you are not expected to understand the technical implications, or terminology.
    - Your procedures may require the referral to be completed by the designated safeguarding lead.
    - Send the email, securely, with a subject of 'Cyber Choices Referral Details' to Cyberchoices@leics.police.uk
    - Always double-check the address is correct before pressing send. If you 'password protect' the document before sending, include your telephone number in the covering email so EMSOU can contact you and obtain the password.

4. *Record the decision to refer to Cyber Choices*
    - All concerns, discussions and decisions made, and the reasons for those decisions, should be recorded in writing, in accordance with your organisation's policy and procedures.

If there are any safeguarding concerns, these should be the primary consideration and you should follow Derby and Derbyshire Safeguarding Children Partnership multi-agency procedures or the Derby and Derbyshire Safeguarding Adults policy and Procedures. Where there are concerns about criminal exploitation due to the individual's enhanced cyber skills, you should refer to the CRE Toolkit, and complete the CRE Risk Assessment.

A Cyber Choices referral does not replace a safeguarding referral.

Upon receipt of the Cyber Choices referral form, the regional Cybercrime Unit at **East Midlands Special Operations Unit (EMSOU)** will:-

1. *Acknowledge receipt of the referral*

2. *Assess the suitability of the referral and undertake regional checks*
    - A crime intelligence check to establish whether the individual is already known to the National Crime Agency or the local Police.
    - A 'desktop' risk assessment, which will include identifying safeguarding or cyber-related issues already known to the Police.

3. *Allocate referral*
    - The referral will be allocated to a Cyber Choices Officer, according to the risk and level of offending.

Upon receipt of the referral, **the Cyber Choices Officer** will:-

1. *Contact the referrer*
    - Acknowledge receipt of the referral.
    - Clarify any information on the referral form and, if required, obtain additional information to help understand:-
        - the individual's IT activity and capability
        - the individual's motivations
        - the individual's background / personal circumstances
        - whether there is an existing neurodiversity diagnosis.
    - Discuss any safeguarding concerns identified.
    - If the referral comes from a school, offer an assembly presentation about the Computer Misuse Act.

2. *Contact other organisations currently working with the individual and/or their family*
    - Inform partners of the involvement of Cyber Choices (if it is proportionate and necessary to do so).

3. *Where the individual is under 18 or identified as a vulnerable adult, contact the parent(s)/guardian(s)/carer(s)*
    - Seek written consent to meet their child.
    - Agree an appropriate location for the initial assessment meeting, which will often be school.
    - Identify who could / should be the additional adult accompanying the individual at the initial assessment. This could be the referrer, teacher, parent/guardian/carer, second Cyber Choices Officer or any other adult, as agreed, but the individual should feel able to speak freely in their presence.
    - Obtain additional information such as:-
        - their knowledge of the individual's computer activity
        - any indicators of activity they may not be aware of.

- Provide advice and information about:-
    - cyber security
    - parental controls.

4. Undertake an initial assessment with the individual as soon as possible

- During the meeting, the Cyber Choices Officer will:-
    - Assess their knowledge of the Computer Misuse Act 1990.
    - Identify what computer equipment they are using.
    - Assess their IT skills and knowledge.
    - Discuss what cyber activity they have been involved in.
    - Establish what online forums they are engaged in.
    - Identify what social media they use.
    - Identify what usernames or tags they use.
    - Understand their motivations and influences.
    - Discuss neurodiversity and any behavioural difficulties they may have.
    - Assess their risk of becoming (further) involved in cybercrime.
    - Assess their risks from the people they are associating with online.
    - Explain the purpose of Cyber Choices
    - Discuss possible actions and interventions.
    - Agree an Action Plan and timescales.
- If the referrer and the parent(s)/guardian(s)/carer(s) are not present at the initial assessment, they will be provided with feedback afterwards.

5. Cyber Choices interventions

- The interventions will be delivered, in the main, by the Cyber Choices Officer.
- Consent for the proposed Cyber Choices interventions will be obtained from the individual and their parent(s)/guardian(s)/carer(s).
- Frequency of contact, and the number of interventions, will be tailored and agreed with the individual.
- A Cyber Choices 'Conditions of Engagement' will be signed by the individual, their parent(s)/guardian(s)/carer(s) and the Cyber Choices Officer.
- The interventions and activities used will be tailored to the individual's needs and skills.
- The type of interventions that could be used as part of Cyber Choices may include, but are not limited to:-
    - Completion of the Cyber Engagement Pack, which includes work on:-
        - The Computer Misuse Act 1990.
        - Consequences of committing cybercrime, both for the perpetrator and their victims.
        - The ethics of cyber security.
        - Appreciating how their advanced cyber skills can benefit them and the wider society.
        - Highlighting potential career opportunities and identifying the entry routes.
        - Identifying legitimate ways to develop their technical skills, such as online training courses.

        - Peer pressure and positive cyber role models.
        - Referring to other support groups, agencies, professionals.
    - Technical cyber interventions, such as:-
        - Testing their technical and problem-solving skills, through cyber security challenges, such as those set by the National Cyber Security Centre.
        - Coding Clubs
        - Immersive Lab licences
        - Other cyber challenges (see Useful Websites).

6. Review of risk

- There will be regular reviews with the individual and their parent(s)/ guardian(s)/carer(s) to assess progress, identify changes in behaviour and review risk.
- The Cyber Choices Officer will constantly review the risks of the individual becoming further involved in cybercrime and any risks posed with people they are associating with online. The risk assessment will consider information provided by the individual, their parent(s)/guardian(s)/carer(s), professionals and police intelligence.
- If any additional safeguarding concerns are identified, safeguarding procedures will be followed and appropriate information shared with partner agencies.
- The level of risk, and on-going issues that present themselves, will determine the:-
    - Type and length of interventions
    - Need for any other partner involvement
    - Need for any enforcement activity
    - Exit strategy.
- If appropriate and consent has been given, the original referrer will be provided with regular feedback on the individual's progress.

7. Discharge

- The Cyber Choices Officer will agree an exit strategy with the Cyber Choices Sergeant at EMSOU.
- The exit strategy and final discharge will be discussed and agreed with the individual and their parent(s)/guardian(s)/carer(s).
- If appropriate and consent has been given, the original referrer will be notified of the discharge from Cyber Choices.
- A final assessment will be conducted to capture the changes in behaviour achieved during the Cyber Choices programme.
- The Cyber Choices Officer will be available for ad hoc advice and information in the future, if required.

A flowchart of the referral process is included at APPENDIX B – CYBER CHOICES REFERRAL FLOWCHART

EMSOU Case Study Examples

Case study one

One of the most high-profile young hackers within the UK went to school in Leicestershire and went on to hack a government agency. There are points in his cyber journey where, if early intervention were offered, it could have diverted him away from offending:-

- At school, he was known by peers and family members to have a high level of interest in computing. He did not take ICT at school and all of his skills were self-taught.
- His interest in hacking developed and he actively sought to increase his skill level at home, with self-taught hacking videos and forums. He was spending a significant amount of time online, often into the early hours of the morning.
- He was expelled from school for another incident, which increased his isolation and difficulty in connecting with people. He started to form friendships online and had better friends in the virtual world, than the physical world. No referral or computer diversion schemes were available at the time, and it is unsure whether the professionals involved (CAMHS and school) knew about his high level of IT ability.
- He became part of an online hacking group and started to gain access to sensitive personal information and began posting it online.

He has engaged with EMSOU to provide the police with resources and learning to prevent others going down the same route.

Case study two

A seven year-old boy, who was autistic, had an obsession with ROBLOX and had 200 ‘friends’ online. There were a number of indicators that resulted in the referral to Cyber Choices:-

- He was learning about binary code and could give you a full history on the Wannacry virus.
- He was contacted online by a ‘friend’ and given ‘co-owner’ rights and, at that point, he shared his account password with his friend. The friend then stole some of his ROBLOX money (actual money) and he felt that he had been hacked. As a result, he then became interested in ‘hacking’ other people’s accounts and learnt, via YouTube, about weak passwords and guessing passwords. He then started to ‘social engineer’ information out of his friends and gained unauthorised access to their accounts to take money.
- This unauthorised access was noticed by school so, along with his vulnerabilities and obsession with computers, they made a referral to Cyber Choices.
- An initial visit was completed with his mother, upskilling her with technical knowledge to keep him safer at home. She was also given a checklist to complete, including contacting their Internet Service Provider (ISP) to obtain higher level of filtering/limiting.

- An initial meeting was held with the boy at school and his capability was assessed. He had an advanced knowledge for his age and, due to his vulnerability, it was imperative to give him guidance and teach him about keeping himself safe to prevent external influence and exploitation.
- A further visit was completed with the boy and his mother to ensure that the messages were taken on board. Low level engagement activities were given to ensure that his cyber interest was harnessed to prevent him from being exploited.

USEFUL INFORMATION

Advice for Parents/Guardians/Carers

Below is some advice you can use to advise parent(s)/guardian(s)/carer(s) on what they can do to support their child:-

- Make sure you know what your child is doing online.
- Monitor what they are doing on the computer by placing all devices, they have access to, in a communal area of the house.
- Who are they communicating with? Can their 'friends' be verified?
- Talk to your child – try to learn about computing with them. You will soon better understand what they are doing and what their ability and risk is.
- Internet Matters will help you understand some of the sites, games or apps they spend time on.
- Moderate the amount of time they spend online. More than four hours a day online is deemed excessive, so encourage other non-computer based activities. Your home broadband can restrict these hours automatically, minimising conflict.
- Discuss the importance of honesty, legality and the consequences of being involved in cybercrime.
- Encourage your child to join a local coding club, which is appropriate for their age and ability.
- Encourage your child to explore the legal and highly rewarding IT careers open to them.
- Complete the Digital MOT to improve your basic cyber security.
- Set up parental controls on all devices, broadband, app stores (Google Play, Apple App Store) and individual apps.
- Read the NCA Cyber Choices parents booklet

Cyber Careers

Cyber security is currently one of the most well-paid, in-demand sectors, but it also offers the chance to forge a career doing something that matters.

Possible careers include coding, engineering, web development, penetration testing, security operations, law enforcement, legal hacking and many more roles, both in the public and private sectors.

So why should people consider a career in cyber security?

- Whatever their skills or interests, there is something for everyone – a number of organisations offer insight days, internships, and apprenticeships.
- It is one of the highest paid industries, due to the increasing demand for talent, so there is an excellent salary from the start and attractive benefit packages.
- Varied career paths provide opportunities for entry level IT technicians to progress their career in more specialised roles within cyber security.
- Talented individuals are in high demand, not just in the UK but also abroad, which means there are opportunities to travel to new places whilst learning new cyber skills.
- Being part of a dynamic industry – never a dull day with the opportunity to keep refreshing skills and expanding their knowledge of the cyber-world.
- Highly transferable skills that can be applied to many industry sectors. As a cyber security professional, they could work for technology giants, such as Google and Facebook, or the UK government, in retail, banking and finance, or in the media.

More information about cyber careers can be found below.

Useful Websites

Careers	
Cyber First	Bursaries and degree apprenticeships offering a different choice after A Levels, or whilst at university.
Cyber Games Careers Fairs	Interactive careers opportunities to give students the chance to meet industry experts, explore potential careers, discover education opportunities and learn about practical next steps.
Cyber Security Challenge UK	Information about how to access a career in cyber security.
GCHQ	Career opportunities at GCHQ.
Inspired Careers	Roles available within the cyber security industry.
UK Cyber Security Council	Cyber security career pathways.

Teaching Resources	
Barefoot	Be Cyber Smart lesson plans and activities for KS1 and KS2.
Cyber Explorers	Resources to introduce 11-14 year-olds to key cyber skills.
East Midlands Cyber Secure (EMSOU)	A series of teaching resources from the police regional cybercrime team.
PHSE Association	Exploring Cybercrime: KS3 Lesson plans from the National Crime Agency.

Cyber Security Training	
Code Club World (part of the Raspberry Pi Foundation)	Free coding games and activities for children.
Codecademy	Online resources to develop coding skills.
Cyber First	A series of short courses (Adventurers, Defenders, Futures and Advanced), available through the National Cyber Security Centre, designed to introduce young people to the world of cyber security.
Cybrary	Online IT and cyber security learning opportunities.
Extended Project Qualification (EPQ) in Cyber Security	A distance learning level 3 qualification in cyber security, accredited by City & Guilds, worth up to an extra 28 UCAS points.
Future Learn	Short Open University courses in cyber security.
Immersive Labs	A platform that hosts modules to deliver e-learning style training around cyber issues.
National Careers Service Skills Toolkit	Details of free IT and cyber security courses.

Safe and Legal Cyber Challenges to test and develop skills (NB - *All the third-party sites listed are publicly available for personal development. They are not endorsed, supported or monitored by law enforcement agencies and so we cannot be held responsible for the content of these sites.)*	
Cyber Centurion	An annual team-based competition, for 12-18 year olds with an interest in cyber, defence, puzzles and code breaking.
Cyber Discovery	A government online extra-curricular programme to master technical skills and security concepts and improve digital skills.
Cyber Games	A series of interactive online games suitable for all ages and levels of technical ability, from the NCA and Cyber Security Challenge UK
Hack The Box	A more advanced site to test penetration skills.
Over The Wire	War games that provide the opportunity to learn and practice security concepts whilst playing.
VulnHub	Tests penetration skills and facilitates the exchange of ideas with thousands of other professionals in the security field.

General information	
East Midlands Cyber Secure	Regional Cybercrime Unit at East Midlands Special Operations Unit (EMSOU))
National Crime Agency	Information about the national Cyber Choices programme

Contacts

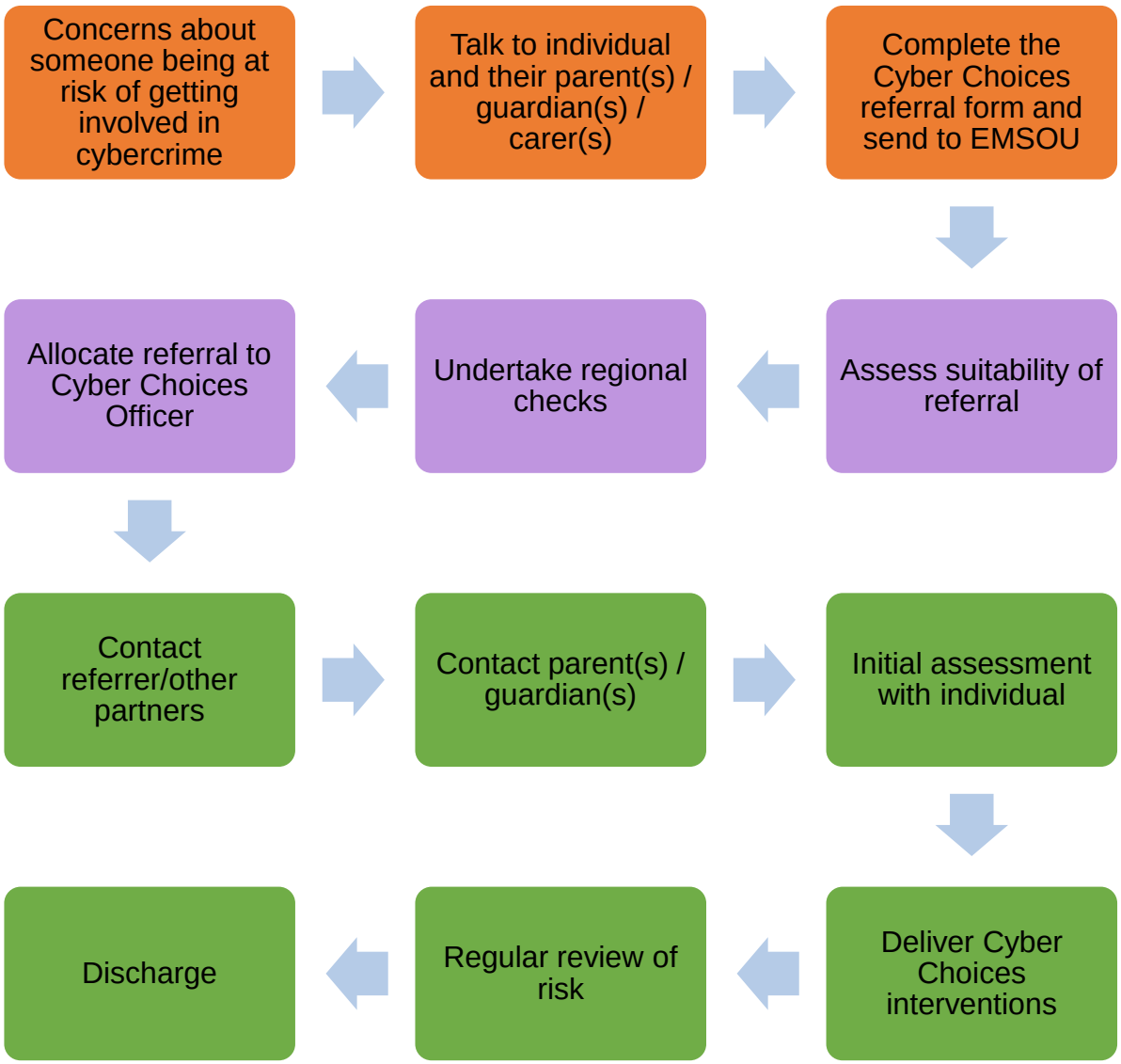
Derbyshire Constabulary Cybercrime Unit	cyber@derbyshire.police.uk
East Midlands Special Operations Unit (EMSOU)	Cyberchoices@leics.police.uk

APPENDIX A – COMPUTER MISUSE ACT 1990

The Computer Misuse Act 1990 makes the following actions illegal:

Offence	• Example of potential unlawful activity
Section 1 - Unauthorised access to computer material (includes desktops, laptops, servers, tablets and smartphones) MAX PENALTY - 2 years in prison	•Without them knowing, you watched your friend put their password into their phone. You then used it to gain access to their phone and download their photos.
Section 2 - Unauthorised access to a computer with intent to commit, or facilitate commission, of further offences MAX PENALTY - 5 years in prison	•Without their permission, you accessed your friend's phone, obtaining their bank login details, so you could transfer money from their account.
Section 3 - Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer MAX PENALTY - 10 years in prison	•You learned, from a YouTube video, how to use a webstresser, or booter tool, to perform a Denial of Service (DoS) attack against a friend, knocking them off an online game, so that you could win. You paid with PayPal, so thought this was probably legal.
Section 3A - Making, supplying or obtaining articles for use in another Computer Misuse Act offence MAX PENALTY - 2 years in prison	•This offence covers the possession of 'malware', but also legitimate software, which you have the intent of using to commit an offence. •You downloaded a programme, which was able to take remote control of a friend's computer, without their knowledge. You didn't get a chance to use it before you were caught.
Section 3ZA - Unauthorised acts causing, or creating risk of, serious damage MAX PENALTY - 14 years in prison but, for damage or threat to human welfare or national security, it is life imprisonment	•You carried out a Distributed Denial of Service (DDoS) attack against a Government department. You did this because you wanted to prove a point. Your attack prevented critical communications, so national security was undermined.

APPENDIX B – CYBER CHOICES REFERRAL FLOWCHART



Responsible agency

Referrer | EMSOU | Cyber Choices Officer

https://www.eastmidlandscybersecure.co.uk/cyber-choices

If you have concerns about cyber-enabled crime, such as youth produced sexual imagery (sexting), cyberbullying, online exploitation, online radicalisation, you must follow existing safeguarding children or safeguarding adult procedures and, where appropriate, make a referral to the relevant local authority.

If you have concerns about the criminal exploitation of vulnerable individuals for their enhanced cyber skills, you must follow existing safeguarding procedures and the CRE Toolkit.

If a child, young person or vulnerable adult is in immediate danger, call the Police immediately on 999.

APPENDIX C – CYBERCRIME DECISION MAKING FOR SCHOOLS (NPCC)