Rothbury First School Safeguarding Newsletter July 2023

WHO TO CONTACT IF YOU HAVE A CONCERN ABOUT A CHILD

If you are worried about a child's safety please do not hesitate to contact the Designated Safeguarding Leads straight away.

The following members of staff are Designated Safeguarding Leads at Rothbury First School
Mrs C Auld
Mrs H Duffield

Our safeguarding governor is
Diane Pringle

They can be contacted on 01669 620283 or via email

For further information on safeguarding at our school, please look on the safeguarding page on the school website.
RFS Safeguarding

DOMESTIC VIOLENCE

Information taken from NSPCC

1 in 4 women and 1 in 6 men will suffer domestic abuse at some time in their lives.

What is domestic violence?

Domestic violence is any kind of abuse that happens between people in a relationship. It can involve threatening, controlling, frightening, bullying or violent behaviour – and may be physically, emotionally, sexually or financially abusive. Children witnessing domestic violence between two adults are also experiencing abuse – and they may be at risk of being abused themselves by the same adult.

Domestic violence between adults could include;

- kicking, hitting, punching or cutting
- rape (including in a relationship)
- controlling someone's finances by withholding money or stopping someone earning
- controlling behaviour, like telling someone where they can go and what they can wear
- not letting someone leave the house
- reading emails, text messages or letters
- threatening to kill someone or harm them
- threatening to another family member or pet.

Living in a home where domestic abuse happens can have a serious impact on a child or young person's mental and physical wellbeing, as well as their behaviour and this can last into adulthood. What's important is to make sure the abuse stops and that children have a safe and stable environment to grow up in.

Being exposed to domestic abuse has serious consequences for children and young people; and it can affect how they feel, think and behave in harmful ways. Thanks to the NSPCC campaign alongside other children's charities and women's organisations and the backing received from supporters around the UK – government agreed to recognise children as victims. The Domestic Abuse Act should mean that they can access the protection and support they need to recover.

Where can victims of domestic violence get support and help?

Refuge

Supports women and children who are experiencing, or have experienced, domestic violence or abuse. You can call their helpline for support, information and advice - including help to access their emergency accommodation.
You can send a message to the helpline using this online contact form (response time within 48 hours, or at a safe time chosen by you).
0808 2000 247

Rape Crisis Centre

Supports girls and women who have experienced rape, sexual violence or sexual abuse at any time.
Find your local crisis centre.
0808 802 9999

Men's Advice Line

Provides support, information and advice for men experiencing domestic violence or abuse.
0808 8010327
info@mensadviceline.org.uk

NSPCC

Information and advice for any adult concerned about the safety of a child.
0808 800 5000
help@nspcc.org.uk

Victim Support

Offers support to anyone affected by crime; not only those who experience it directly, but also their friends, family and any other people involved.
0808 168 9111

Family Rights Group

Provides support, information and advice to parents whose children are involved with, or in need of, social services because of safety or welfare concerns - as well as parents and relatives of children in the care system.
Phone: 0808 801 0366

ONLINE SAFETY - CYBER RESILIENCE

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many issues which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

12 Top Tips for

BUILDING CYBER RESILIENCE AT HOME

As a society, we're increasingly using technology and tech services in the home. Digital assistants which can adjust the heating or turn lights on and off; streaming services for shows and movies on demand; games consoles; smart speakers; phones; laptops ... the list goes on. As we introduce each new gizmo to our homes, however, we increase the level of threat from cyber criminals. It's essential, therefore, that we learn to become more cyber resilient in relation to the devices and digital services that the people in our household use.

WHAT IS 'CYBER RESILIENCE?'

*Cyber resilience focuses on three key areas: reducing the **likelihood** of a cyber attack gaining access to our accounts, devices or data; reducing the potential **impact** of a cyber incident; and making the **recovery** from a cyber attack easier, should we ever fall victim to one.*

1. PASSWORDS: LONGER AND LESS PREDICTABLE

The longer, less common and predictable a password is, the more difficult it becomes for cyber criminals to crack. The National Cyber Security Centre's 'three random words' guidelines are ideal for creating a long password which is easy to remember but hard to guess.

2. AVOID RE-USING PASSWORDS

When you use the same password across different logins, your cyber resilience is only as strong as the security of the weakest site or service you've signed up for. If cyber criminals gain access your username and password for *one* site or service, they'll definitely try them on others.

3. USE A PASSWORD MANAGER

A good way to juggle different passwords for every site or service you use is to have a password manager. This software stores all your passwords for you, so you simply need to remember the master password. LastPass, Dashlane, 1Password and Keeper are all excellent password managers.

4. BACK UP YOUR DATA

Keep a copy of your data using OneDrive, Google Drive or another reputable cloud-based storage solution. If it's extremely important or sensitive information, you could even decide to keep more than one back-up version – by saving it to a removable USB drive or similar device, for example.

5. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

Multi-factor authentication is where you need access to your phone (to receive a code, for example) or another source to confirm your identity. This makes it far more difficult for cyber criminals to gain entry to your accounts and your data, even if they *do* manage to get your username and password.

6. CHOOSE RECOVERY QUESTIONS WISELY

Some services let you set 'recovery questions' – such as your birthplace or a pet's name – in case you forget your password. Take care not to use information you might have mentioned (or are likely to in future) on social media. More unpredictable answers make cyber criminals' task far harder.

7. SET UP SECONDARY ACCOUNTS

Some services provide the facility to add secondary accounts, phone numbers and so on to help with potentially recovering your account. Make sure you set these up: they will be vital if you're having trouble logging in or if you're trying to take back control of your account after a cyber attack.

8. KEEP HAVING FUN WITH TECH

Consider our tips in relation to the gadgets and online services your household uses. Protect yourself and your family, and don't let the bad guys win: devices are not only integral to modern life but also a lot of fun – so as long as you keep safety and security in mind, don't stop enjoying your tech.

9. CHECK FOR BREACHES

You can check if your personal information has been involved in any known data breaches by entering your email address at www.haveibeenpwned.com (yes, that spelling *is* correct!). It's useful if you're worried about a possible attack – or simply as motivation to review your account security.

10. CHANGE DEFAULT IOT PASSWORDS

Devices from the 'Internet of Things' (IoT), such as 'smart' home appliances, are often supplied with default passwords. This makes them quicker to set up, but also less secure – criminals can identify these standard passwords more easily, so change them on your IoT devices as soon as possible.

11. KEEP HOME DEVICES UPDATED

Download official software updates for your household's mobile phones, laptops, consoles and other internet-enabled devices regularly. Security improvements and fixes are a key feature of these updates – so by ensuring each device is running the latest version, you're making them more secure.

12. STAY SCEPTICAL

Cyber criminals commonly use various methods, including emails, text messages and social media posts. Be cautious of any messages or posts that are out of the ordinary, offer something too good to be true or emphasise urgency – even if they appear to come from someone you know.

Meet Our Expert

Gary Henderson is the Director of IT at a large boarding school in the UK, having previously taught in schools and colleges in Britain and the Middle East. With a particular interest in digital citizenship and cyber security, he believes it is essential that adults and children alike become more aware of the risks associated with technology, as well as the many benefits.

Source: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-word | https://haveibeenpwned.com

National Online Safety® #WakeUpWednesday