# Forres Sandle Manor (Non-Academic) Policy

| Policy Title                           | E-Safety Advice for Parents |
|----------------------------------------|-----------------------------|
| Policy Lead (Appointment (& Initials)) | Deputy Head Pastoral (JC)   |
| Date of Last Review                    | September 2019              |
| Date of Next Review                    | September 2020              |

# **E-SAFETY ADVICE FOR PARENTS**

The Internet is a great place for your children to have fun and keep in touch with family and friends. Because of the huge amount of information available online, the potential for educational benefit to your family from legitimate online sources is nearly unlimited. On the other hand, just as you protect your children from dangers in the "real" world, you should be aware of the possible dangers that tempt naive and trusting children, especially teenagers, into dangerous situations in the "online" one. Becoming educated about technology and striving to open and maintain lines of communication with your children is just as critical as teaching young children to look before they cross the road and older ones to become responsible drivers. Your job to educate and protect your children supersedes any feelings they may have regarding their rights to privacy!

#### WHAT ARE THE POSSIBLE DANGERS?

- Accessing inappropriate web sites: A few examples: pornography; extremist activities; hate groups.
- **Bullying, harassment, and character defamation** in the public arena of the Internet, by e-mail and social networking, can be cruel, vicious, degrading and very damaging to children and teens.
- Sexting or Youth Produced Sexual Images: refers to the sharing of naked or 'nude' pictures or video through mobile phones and the internet. It also includes underwear shots, sexual poses and explicit text messaging. While sexting often takes place in a consensual relationship between two young people, the use of Sexted images or texts in revenge following a relationship breakdown is becoming more commonplace. Sexting can also be used as a form of sexual exploitation and take place between strangers.
- Contact with undesirable persons: most common via social networking, e-mail or instant messaging. These people take advantage of a child's insecurities to befriend them.
- Scams, fraud and identity theft: Internet users may unwittingly fall victim to criminal scams that begin by asking for passwords, credit card information, addresses and other personal information in a way that appears to be legitimate.
- Sales: While there are many ethical e-commerce sites and sellers doing business on the Internet, there are numerous fraudulent operators misrepresenting merchandise or using an e-commerce site to collect credit card information. As with television, the

- Internet is being used for aggressive marketing campaigns aimed at young consumers. Buyers must be very careful purchasing from Internet auction sites. If it's too good to be true, it's probably a scam.
- **Computer issues**: Viruses, worms, spyware, adware and some peer to peer software may cause your computer or software to malfunction or compromise your security and privacy. Install and use an antivirus program and a firewall. You should also install and regularly run software that searches your computer for spyware and adware. Download and install only reputable software programs.

# HOW CAN I HELP MY CHILD AVOID RISKY SITUATIONS AND MAKE SENSIBLE DECISIONS?

When raising the awareness of e-Safety we would encourage families to focus on:

- The range of different ways children and young people use and access technology e.g. mobile phones, games consoles, tablets, e-readers and apps etc. not just laptops and computers.
- The many positive uses of technology as otherwise e-Safety can easily become frightening and scaremongering so be aware that the vast majority of interactions and experiences on the internet are positive!
- The importance of developing risk awareness and risk management by children and young people (according to their age and ability) and resources parents/carers can use to help discuss online safety.
- Discussing the various risks and issues such as responsibility, trust and consent.
- Practical tips for e-safety in the home such as using filters, parental controls, creating appropriate user profiles and home computer security.

The following is guidance from CEOP (Child Exploitation and Online Protection): **Location** 

- Place your computer in an open area of your home where you can easily supervise your child's computer activities.
- Consider locating your computers and laptops in a family area where children's
  online activity can be monitored or supervised. Always supervise the use of
  webcams and any applications or devices which allow voice or video chat. Also
  consider the use and location of other devices your child uses which allow internet
  access such as mobile phones and games consoles.
  - Visit <a href="https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parents-guide-technology">https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parents-guide-technology</a> for safety information about consoles and devices.

#### **Online Safety**

- Install antivirus software, secure your internet connection and use Parental Control functions for computers, mobile phones and games consoles to block unsuitable content or contact.
- Check with your current provider to find out what services they offer. Purchase monitoring and filtering software that allows you some control over computer use

- Parental controls are not just about locking and blocking, they are a tool to help you
  set appropriate boundaries as your child grows and develops. They are not the
  answer to your child's online safety, but they are a good start and are not as difficult
  to install as you might think. Service providers are working hard to make them
  simple, effective and user friendly.
- Always remember that parental control tools are not always 100% effective and sometimes unsuitable content can get past them, so don't rely on them alone to protect your child.

### **Know What Connects To the Internet and How**

Nowadays even the TV connects to the internet. Your child will use all sorts of devices and gadgets; make sure you are aware of which ones can connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection or a neighbour's Wi-Fi? This will affect whether your safety settings are being applied.

#### Be Involved in Your Child's Online Life

Think about what they might see, what they share, who they talk to and how long they spend online. It is important to continue to discuss boundaries so that they evolve as your child's use of technology does.

- Discuss as a family how the internet will be used in your house.
- Establish clear and reasonable rules for computer use in your home and outside your home. Limit the time and the hours of the day your child can participate in online activities. Make sure you create, explain and implement consequences for breaking the rules.
- Consider what information should be kept private (such as personal information, photos etc.) and decide rules for making and meeting online friends. For many of today's young people there is no line between the online and offline worlds. Young people use the internet to socialise and grow, and just as you guide and support them offline, you should be there for them online too. Talk to them about what they're doing, if they know you understand they are more likely to approach you if they need support.
- Internet accounts and profiles should be in your name and you should control
  passwords and screen names. Help your child choose a screen name that is
  nondescript. Do not allow children to have personal profiles because these can often
  be easily accessed by undesirable individuals.

# **Keep Up-To-Date with Your Child's Development Online**

Be inquisitive and interested in the new gadgets and sites that your child is using. It's important that as your child learns more, so do you.

Know who your children exchanges e-mails with. If they have a "friends list", check it
often for changes.

- Know your child's friends and talk to their parents about computer use in their homes. Be aware of other computers outside of your home that your child may be using.
- Keep the lines of communication open with your child. Be supportive of the educational
  and fun uses of technology and spend time exploring the Internet with your child. Work
  to establish an atmosphere of trust within your family, encouraging your children to tell
  you about their online activities.

### Use the NSPCC 'Share Aware' website:

- This provides information to help your child stay safe on social networks, apps and games. It provides information of what other parents think about the main social media apps, their suggested age rating and details on privacy and safety settings with a useful 'netaware' tool.
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/

#### Watch 'Thinkuknow' Films To Learn More

- The 'Thinkuknow' programme has films and advice for children from five all the way to sixteen. Your child may have seen these at school, but they can also be a good tool for you to find out more about what young people do online and some of the potential risks.
- Discuss using strong passwords with your child so they understand how they can
  protect their online accounts. It's important they know they need to keep their
  passwords safe and not share them with anyone or use the same password for several
  accounts. If your child's account is "hacked" or compromised then make sure they
  change their password and report any concerns or suspicious activity.

Check how secure your passwords are here: <a href="http://howsecureismypassword.net/">http://howsecureismypassword.net/</a>
For more advice on using strong passwords visit <a href="http://tinyurl.com/Getsafeonlinepassword">http://tinyurl.com/Getsafeonlinepassword</a>

Help your children understand...

- What personal information is and why it should not be given.
- What is being posted on a web site or discussed online can affect a person's privacy and reputation and often cannot be deleted or removed.
- The importance of not responding to unsolicited, offensive or unpleasant e-mail or chat.
- While they may feel "alone" online, they are not. People can find out who they are and where they are by taking advantage of the natural tendencies of children and teens to be trusting and open.
- What sexting is and what trust and consent in a healthy relationship looks like
- What they read or see online is not all factual or reliable. Encourage a cautious approach to online "information".
- Recognize that chat rooms and social networking can be dangerous. Do not allow your child to visit chat rooms or, at the very least, restrict them to age and subject appropriate chat rooms only and monitor their activity. Chat services that provide Page 4 of 6

monitors are generally safer than unmonitored chat rooms, but parental supervision is essential in any case.

# Tell your children...

- To tell you immediately if they are threatened, scared or made uncomfortable by someone or something online (be sure you respond in a helpful and calm manner).
- Never give out their own or their friends' names, addresses, phone numbers, parents' names, school names, or other personal information.
- Never agree to personally meet someone they met online.
- Never send photographs online without your permission.
- Never fill out forms or questionnaires online without your permission.
- Not to enter areas that charge for services without your permission.

## WHAT WARNING SIGNS SHOULD I WATCH FOR?

- Your child spends a great deal of time on the Internet or is online late at night.
- Your child changes the computer screen when you enter the room.
- Your child becomes uneasy or defensive when you are close to their online activity
  or discussing online behaviour (If you see your child type POS this is a red flag. It
  means "parent over shoulder").
- There are unusual charges on credit card statements or phone bills. Be especially
  alert to charges with seemingly benign identification. Pornographers and con artists
  are careful not to attract attention by using descriptive names.
- Your child has a sudden influx of cash or gifts.
- You notice changes in your child's behaviour or habits (secretiveness, inappropriate knowledge, changes in interests, sleeping problems, etc.).

# WHAT SHOULD I DO IF I KNOW OR THINK MY CHILD IS BEING EXPOSED TO POTENTIALLY RISKY SITUATIONS?

**Know what to do if something goes wrong**. Just as in the offline world, you want to help your child when they need it. Therefore, it is important to know when and how to report any problem.

- Communicate with your child and be involved. Be non-judgmental as you encourage your child to answer your questions and discuss your concerns.
- If your child is involved in online bullying or harassment, either as a perpetrator, victim or bystander, engage in a discussion of ethics, kindness and respect. Talk about the legal realities of criminal arrest or civil litigation in extreme cases of cyberbullying. Your child's role in the activity will determine how you respond.
- If threatening or pornographic material is received by your child, save it. If you can identify the company, report the incident to the sender's Internet Service Provider (ISP).
- If you have any concerns or queries, please do not hesitate to contact the school.

- Report any content or activity that you suspect may be illegal. You can report your concerns using one of the following contacts.
  - Children's Social Care: 08458 247247
  - Hampshire Police: 101
  - CEOP: Visit www.ceop.police.uk and use the "Click CEOP" reporting button

# **FURTHER LINKS & RESOURCES**

Further advice and information through the following organisations:

- DfE advice on Sexting: See Annex C <u>DfE/Sexting</u>
  - Safer Internet Centre <a href="https://www.saferinternet.org.uk/advice-centre/parents-and-carers">https://www.saferinternet.org.uk/advice-centre/parents-and-carers</a>
- Think you know <u>www.thinkuknow.co.uk</u> – Visit the "Parent/Carer" Section and use the "Click CEOP" button to seek advice and report online abuse.
- Childnet Services <a href="http://www.childnet.com/resources/know-it-all-for-parents">http://www.childnet.com/resources/know-it-all-for-parents</a> an interactive guide about online safety.
- Get safe online <a href="https://www.getsafeonline.org/protecting-yourself/passwords/">https://www.getsafeonline.org/protecting-yourself/passwords/</a> 
   Free up-to-date Security advice including using complex passwords and managing hacked accounts.
- The Anti-Bullying Alliance www.anti-bullyingalliance.org.uk/.
- The Diana Award <a href="www.antibullyingpro.com">www.antibullyingpro.com</a>.
- The Parent Zone <u>www.theparentzone.co.uk.</u>
- www.bbc.co.uk/onlinesafety.