The Ryleys

Girls & Boys Preparatory School

The Ryleys School E-Safety/ Online Policy

Monitoring: Deputy Headteacher
Named Person Responsible: S.Kirkbright
Reviewed: April 2019
Policy Review Date: April 2022

Scope

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positive and exciting opportunities, but also challenges and risks.

The use of the latest technology is actively encouraged at The Ryleys but with this comes a responsibility to protect both pupils and the school from abuse of the system.

What is the policy?

Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy, Anti-Bullying Policy, Behaviour Policy and Staff Code of Conduct.

Who is responsible?

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

All staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the students. Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy.

The role of parents in ensuring that students understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

- support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures.
- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour.
- encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

If parents have any concerns or require any information about online safety, they should contact the school.

Assessment of risks

- The school currently does not allow pupils free access to mobile phones, ipads and laptop computers this limits risks posed personally via global networks such as the internet.
- There is a secured wireless network within the school and this means the potential threat to security and access by unauthorised personal is minimised.
- Pupils access computers in the ICT rooms, through a secure, passworded connection to the school network.
- Staff have a username and passworded account, with access and allowance limitations imposed.
- The school internet service is firewalled and secured.
- Pupils have internet access, within lessons, but are prohibited from using games.
- Users are prevented from downloading executable files.
- All web activity is monitored and personal browsing histories kept.
- School web and email settings are set at the highest software security levels.

Education

The safe use of Technology is integral to the School's ICT curriculum. Students are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS in the following ways:

- Children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment.
- Children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology.
- Children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral (P.S.H.E.) activities.

Lesson and activities are designed to teach pupils:

- About the risks associated with using the Technology and how to protect themselves and their peers from potential risks.
- To be critically aware of content they access online and guided to validate accuracy of information. How to recognise suspicious, bullying, radicalisation and extremist behaviour.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.
- How to report cyberbullying and/or incidents that make students feel uncomfortable or under threat and how the School will deal with those who behave badly.

The Ryleys computer system provides internet access to pupils and staff. This RUIS will help protect pupils, staff and the School by clearly stating what is acceptable and what is not.

Responsible Internet Use Statement (RIUS)

1. Access must only be made via the user's authorised account and password, which must not be given to any other person.
2. School computer and internet use must be appropriate to the pupil's academic education or to staff professional activity.
3. Copyrights and intellectual property rights must be respected.
4. Users are responsible for email they send and for contacts made.
5. Emails should be written carefully and politely. As messages may be forwarded, email is best regarded as public property.
6. Anonymous letters and chain mail must not be sent or forwarded.
7. The use of public chat rooms is not allowed.
8. Only games to enhance lessons may be used during school hours.
9. No internet games may be accessed.
10. Only use the URL bar with staff permission.
11. Users must log off after use, do not leave a computer logged in and unattended.

Email Rules

- Never reply to unpleasant or unwanted emails.
- Never give your email address to anyone except close family and friends.
- Don't accept emails or open files from people you do not know.
- Do not click on any links or open any email into the full window if you are unsure of the sender or content.
- Visit **www.thinkuknow.co.uk** to ensure you know how to be safe.
- Report abuse at **www.ceop.gov.uk/**

Web Rules

- Do not use the URL bar unless permission is given.
- Do not click on links unless you are certain what they are.
- Report to a teacher if you find a dubious web page as this will appear in your history.

Report any concerns immediately. www.thinkuknow.co.uk and **www.ceop.gov.uk/**

Procedures for dealing with incidents of misuse

Staff, students and parents are required to report incidents of misuse or suspected misuse, including incidents of sexual harassment via mobile or smart tech, to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures. All incidents will be dealt with in line with the above policies.

Misuse by students

- Anyone who has any concern about the misuse of Technology by students should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.
- Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy).

Misuse by staff

- Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.
- If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

Online Safety

Managing Online Risks

- which children are more vulnerable
- what we can do as individuals and parents
- what we should teach children and young people.

Which children are vulnerable?

The reality is that no one is really sure which children are vulnerable because there is so little research on the issue.

A 2012 seminar pulled together the results of what evidence exists to identify which children are likely to be more vulnerable online. They wanted to use the findings to develop robust harm-prevention policies for children's internet use.

Their findings discovered that, whilst it is supposed that children deemed as vulnerable offline are more likely to be vulnerable online may carry some weight, it is vital to take into account a number of other factors which contextualise when, why and how children may be at risk online.

The four Cs

They say there are four Cs for potential risks facing children:

1. Content
Being exposed to harmful material.

2. Contact
Engaging with people who may not be who they say they are and/or may have ill intent. These may, occasionally, be sexual predators, attempting to groom children, potentially with the aim of meeting them offline. They may also be people who intend to threaten, intimidate or bully.

3. Conduct
The child or young person is the one displaying the inappropriate sexual or bullying behaviour or the victim of someone else's behaviour.

4. Commercialism
Being exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

These four Cs come into play at different stages of a child's development and so vulnerability is not a static issue but one that needs to be understood in the broader context of children's lives and their stage of emotional, psychological and physical development.

At the moment, there is no single or simple definition of vulnerability.

Many factors combine to render some children vulnerable to online risk, under particular circumstances, and with diverse consequences.

Most children begin their online life as risk takers, led by curiosity and the ability to simply download/install apps or visit websites. However they will only find themselves in danger as a result of their illegal or inappropriate online behaviour.

Spectrum of Vulnerability

Highly Vulnerable **Risk Taker** **Most Resilient**

The plan should always be to encourage children and young people to become most resilient through –

1. Talking to children and young people
2. Getting involved with what they are doing online
3. Developing awareness and understanding of young people's online behaviours and habits

To support children you must first understand their online behaviours in order to recognise the risks they face. So, if you can describe and explain risk you are in a better position to minimise it and drastically reduce possible harm.

There is very good evidence that children's vulnerabilities online may be related to the nature of the online services they use, the contacts they make, the content that they view, their own or others' risky behaviours and the commercialism they encounter.

There is still much work to be done to understand when, why and how children become vulnerable.

It was mentioned earlier that, although it is apparent that certain groups of children identified as vulnerable offline will also be vulnerable online, this isn't always the case.

The findings shared at the seminar showed that the stage of development of children and young people is a significant factor in determining their online risk – especially children entering puberty.

Safeguarding children and young people is everyone's business.

Where there are concerns about the wellbeing of a child, in addition to considering the traditional forms of abuse (physical, emotional, sexual abuse and neglect), also factor in the wide range of harms that can come via the internet and that offline and online activities are often intertwined.

Also be mindful that some children and young people can pass through several stages of potential vulnerability depending on their online interactions, so it pays to be vigilant to their internet use, whatever the age of the child.

One of the concluding findings of the seminar was that "the more adults around children make themselves emotionally available to them, the more children feel they can confide in them that they have, or are being, harmed".

What we can do:

In general - 'Get Involved'

- What devices/apps are they using, do they allow online interaction?
- Be aware of what young people are doing online.
- Be 'friends' with your children on Facebook and other social networking sites.
- Talk to them and ask what they are doing.
- Use the parental controls on the operating system.
- Speak to your internet service provider about how you can filter internet access (there is more information about this in the Resources tab).

What we should teach children and young people

1. Set privacy settings and guard your information: Address; phone numbers; school; city or town; parent's workplace; passwords.
2. Guard your information: Technology can share information without knowledge; for example, turn off synchronisation on Android devices, turn off location services and switch on when required.
3. Limit time online: Log off and play; take time for family and proper face-to-face time with friends.
4. Friend or foe? Never schedule offline meetings with 'online only' friends; tell parents if anyone tries to meet you offline; not everyone is who they say they are.
5. Communicate: Talk about it if someone has upset you; stay away from 'adult only' sections of the internet; tell your parents about anything that makes you uncomfortable; do not believe everything you see - just because it is on the internet doesn't mean it is true.
6. Safety with webcams: Never do random chat (sites like Chatroulette); only chat with family and friends; never do anything on the webcam you wouldn't want up on the screen; think before uploading video responses.
7. Time and place: Carefully consider whether to use geolocation (showing people exactly where you are) on social networks or games. Ask parents' permission before using it; do not use the internet for personal purposes at school or any place you visit regularly; check your privacy settings.
8. Be 'scam smart': Don't open strange emails; beware of 'free' downloads that could hide viruses or spyware.
9. Don't be a 'pirate' (eg access music, videos or films illegally); don't use peer-to-peer file sharing as it leaves you open to viruses, spyware and identity theft.
10. Teamwork: Help your parents to protect you; help each other; communicate; cooperate; know when to log off.

Guidance on online bullying specifically for children.

- Don't respond.
- Don't retaliate.
- Talk to a trusted adult.
- Save the evidence.
- Block the bully.
- Be polite.

- Don’t be a bully.
- Be a friend not a bystander.

Guidance for adults.

- Listen and take the child seriously.
- Make sure the child is safe and feels safe.
- Don’t overreact.
- Encourage the child not to retaliate.
- Gather the facts and save the evidence.
- Get the child to help solve the problem.
- Teach self-esteem and resilience.
- Talk to the child’s school if there are links with the bullying.
- Encourage the child to reach out to friends.