e-Safety Policy

INTRODUCTION:

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children's Act 2004, it is the duty of all organisations to ensure that children and young people are protected from potential harm both within and beyond the organisation environment. Therefore, the involvement of children, young people and parent/carers is also vital to the successful use of online technologies.

AIMS:

This policy aims to explain how parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'e-Safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside the organisation.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or children and young people, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the boundaries of the organisation.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

ROLES & RESPONSIBILITIES:

Name of organisation: **Green Room Music Theory**

e-Safety: Safeguarding Lead and Deputy Responsibilities
The responsibility of managing e-Safety can be demanding and challenging, and must therefore be appointed at managerial/committee level to personnel who are available when we are operational. (This will normally be the same person who will lead on child protection, unless your organisation has a lot of technology based activities, in which case you may wish to include an IT expert from your organisation who will liaise with the lead person for child protection).

Our lead is:

Rhiannon Bennett

Contact details: rhiannonbennett@greenroomplace.com

OUR e-SAFETY CODE OF CONDUCT:

We expect everyone in our organisation to agree and sign up to our code of conduct:

I will:

1. Use the internet and other forms of communication in a sensible and polite way.
2. Only access websites, send messages or access and use other resources that will not hurt or upset anybody.
3. Seek permission if I want to use personal information or take photographs of other people.
4. Report any concerns to the lead or deputy person for E-Safety immediately.
5. Be clear that I cannot maintain confidentiality if there is a concern about the welfare of a child or young person.

WHAT ARE THE RISKS?

There are many potential risks for children and young people including:

- Accessing age inappropriate or illegal websites.
- Receiving unwanted or upsetting text or e-mail messages or images.
- Being "groomed" by an adult with a view to meeting the child or young person for their own illegal purposes including sex, drugs, or crime.
- Viewing or receiving socially unacceptable material such as inciting hatred or violence.
- Sending bullying messages or posting malicious details about others.
- Ignoring copyright law by downloading music, video or even homework cheat material.

WHAT ELSE MIGHT BE OF CONCERN?

A child or young person who:

- Is becoming secretive about where they are going to or who they are meeting.
- Will not let you see what they are accessing on-line.
- Using a webcam in a closed area, away from other people.
- Accessing the web or using a mobile or PDA (Personal Data Assistant) for long periods and at all hours.
- Clears the computer history every time they use it.
- Receives unexpected money or gifts from people you don't know.

An adult who:

- Befriends a child/ren or young person/people on the internet or by text messaging.
- Has links to children or young people on their Facebook or other social network site; especially if they work in a position of trust such as a sports coach or youth worker.
- Is secretive about what they are doing and who they are meeting.

WHAT DO I DO IF I AM CONCERNED?

If you have any concerns speak to the lead or deputy person for e-Safety immediately.

CONTACTS FOR REFERRING:

If the concern is about:

- A child being in imminent danger, ALWAYS **DIAL 999 FOR THE POLICE.**
- The welfare of a child, ring Lincolnshire County Council's Customer Service Centre on 01522 782 111 or access what to do by going to http://moderngov.southkesteven.gov.uk/documents/s16717/Appendix%20B%20-%20Safeguarding%20Children%20Procedures.pdf
- A known person's sexual behaviour or intentions ring the local children's social care services.
- A person who has a "duty of care" in the organisation, ring the local children's social care services. The LADO (Lead Authority Designated Officer) will oversee and advise upon any following procedures.
- An unknown person's sexual behaviour or intentions, report at www.ceop.gov.uk (Child Exploitation and Online Protection Centre).
- Harmful content, including child sexual abuse images or incitement to racial hatred content contact www.iwf.org.uk

REMEMBER:

1. DO NOT DELAY.
2. DO NOT INVESTIGATE.
3. ISOLATE ANY EQUIPMENT AND PREVENT FURTHER USE OF AN ONLINE ACCOUNT.
4. MAKE CAREFUL RECORDING OF ANYTHING YOU OBSERVE OR ARE TOLD.
5. SEEK ADVICE FROM THE LEAD OR DEPUTY PERSON FOR e- SAFETY.
6. REFER IMMEDIATELY.

MINIMISING THE RISKS:

We will:

- Talk to children and young people about what they are accessing on line.
- Keep the computer/s in a general space where we can monitor what is going on.
- Explain the risks of giving out personal details online.
- Talk about how people can be anyone they want to be online: by using misleading emails, photographs of other people, telling lies about their age, school, hobbies.
- Encourage children and young people to think carefully about which photographs or videos they use on line this material can be used and tampered with by other people, or they may not be appropriate.
- Advise children and young people to only text, chat or webcam to people they know for real.
- Talk about how to identify SPAM/SPIM messages or junk mail and how to delete them. This also applies to messages from people they do not know, or opening attachments.
- Discuss how people hide their identities online and the importance of never meeting new online "friends" for real.
- Make sure children and young people understand they can talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
- Look on the internet together for information about how to deal with, or report, problems.
- Talk about how, when information or images get onto the net, they can never be erased or retrieved.

CCTV:

To comply with both the Data Protection Act 1998 and the Information Commissioner's CCTV Code of Practice, all organisations using CCTV for security and safety purposes must publicly declare that they are doing so. The organisation should have erected a sign to inform members of the public that they are entering a surveillance area and to display the following key information.

- The name of the organisation and individuals responsible for the CCTV system.
- The contact details of who is responsible for the system.
- The purpose of the CCTV system.

The organisation must ensure that all images recorded through the CCTV system are fully traceable with the date, time, recording device and person responsible for recording all detail in a secure log for audit trail purposes. A robust and thoughtful collection of Standard Operating Procedures should be in place to govern the day to day operation of the CCTV system. For data security purposes a restricted number of staff should have access to any images and recordings held by the organisation.

RESOURSES:

The organisation:

- Can use the Childnet International 'KnowITAll for Parents' CD/online materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community.
- Ensure that skills around internet use are offered as part of the follow-up training for parents/carers so they know how to use the tools their children and young people are using.
- Endeavour to provide access to the internet for parents/carers so that appropriate advice and information can be accessed where there may be no internet at home, subject to arrangement.

POLICY:

This policy was agreed and disseminated and will be reviewed annually or when there are substantial organisational changes or an e-safety incident.

Policy Review Date: May 2022

SIGNED:……

Safeguarding Lead: Rhiannon Bennett

PLEASE ENSURE YOU NOW READ THE E-SAFETY FLOW CHART BELOW

Guidance on Responding to E-Safety Incidents

In the event of an e-safety incident, a clear and defined action document is invaluable to a school. This guidance should be available to all members of staff, ensuring that the correct steps are followed and the right persons/authorities are notified. Although the specific procedures may vary for each school, the flowchart below is a helpful starting point in understanding how to respond to an e-safety incident.

Top Tips

- Carry out a staff debrief after any e-safety incident
- Always review your school's e-safety policy followng an incident and make appropriate changes if needed
- Encourage an open-door policy to ensure all staff and students feel comfortable reporting any problems
- Record all steps taken to resolve the incident

An e-safety issue is identified/reported

Establish the severity of the incident

Is the material accessed or the actions performed illlegal?

No

Who should the e-safety issue be reported to within the school?

It may be that different people need to be informed according to the degree of the incident:

- Safeguarding/E-safety co-ordinator (always)
- Class teacher (when appropriate)
- Senior leader or headteacher (severe)
- School Child Protection Officer (very severe/raises concerns for child's welfare)

How should the school respond to an e-safety incident?

Depending on the severity of the material accessed/actions perfomed, the following response/s may be appropriate:

- Website/webpages containing the material are blocked via the school's content fltering system
- Any inappropriate content submitted by a pupil is evidenced and removed
- The parents of the student/s involved are notified
- Warning/sanctions are given to the student/s, if appropriate
- Whole-class/or one-one discussions performed with pupils

How should the school move forward after an e-safety incident?

- Ensure all details are recorded and any evidence is preserved
- If needed, provide report of incident to relevant authority
- Review current e-safety policy and implement any necessary changes in order to minimise the chances of the same issue recurring

Yes

What risk is posed to the pupil involved?

If an immediate risk is posed, the following steps are advised:

- A member of staff reports the situation to the Child Protection Team
- Organise a procedure meeting
- Secure all available evidence
- Allow the authorities to complete their investigation and take the necessary steps once it has concluded

If the child does not face immediate risk;

- Report the situation to the Child Exploitation and Online Protection Unit (CEOP)
- Organise a procedure meeting
- Secure all available evidence
- Await response from CEOP and act accordingly once received

Are illegal materials confirmed by relevant authority?

No

Yes

Refer to police for advice on how to proceed

Continue to monitor the situation for any potential devolpments/recurrences - especially pertinent in cases of cyberbullying.

Helpful Websites

www.thinkuknow.co.uk
www.kidsmart.org.uk
www.iwf.org.uk
www.cybersmile.org
www.childnet.com
www.e-safetysupport.com

exa education