BIRKENHEAD
SCHOOL

E-Safety Policy and Code of Practice

Links with other policies:

- Safeguarding Children - Child Protection
- Anti-bullying
- Behaviour Policy
- Safer Recruitment
- Staff code of Conduct
- Health & Safety
- Behaviour Policy

Why have an E-safety Policy?

The use of the Internet as a tool to develop learning, understanding and communication has become an integral part of school and home life. There are always going to be risks in using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children and staff use these technologies. Whilst the School acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to our policy to ensure students are continued to be protected.

Aims

- To outline the roles and responsibilities of staff, students and parents.

- To ensure the safeguarding of all students within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.

- To ensure all users are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.

- This policy aims to inform how parents/carers and students are part of the procedures and how students are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'E-Safety' is used to encompass the safe use of all on-line technologies in order to protect students and adults from potential and known risks.

Roles and responsibilities of the School

It is important to emphasise that we are all responsible for E-Safety and our specific responsibilities are outlined below:

Governors

- It is their overall responsibility to ensure that there is an overview of E-Safety (as part of the wider remit of Safeguarding Child Protection) across the school and that they promote and report on E-Safety developments and their links with the school development plan/ICT development plan, safeguarding child protection, and other policy changes.

- The Governing Body has appointed an E-Safety governor who will challenge the school about having appropriate policies, procedures, staffing responsibilities and ICT security systems.

Network Manager

- Implements agreed policies, procedures, staff training, and curriculum requirements and take a responsibility for ensuring E-Safety is addressed in order to establish a safe ICT learning environment.

- Ensures that all adults in the school and parents are aware of the filtering levels and why they are there to protect students.

- Ensures that the filtering levels on all equipment are appropriate for our students and are set at the correct level.

- Ensures that any concerns are reported to the designated safeguarding lead.

- Keeps a log of incidents for analysis to help inform future development and as part of the school's safeguarding procedures.

  Ensures there is appropriate anti-virus software and anti-spy software in place on all school equipment and that this is reviewed and updated on a regular basis.

- Reports accidental access to inappropriate materials to the ICT technical manager of the ISP and or filtering service so that inappropriate sites are added to the restricted list.

- Responsible for the transparent monitoring of the Internet and on-line technologies. For example, any student or staff files may be accessed by the network manager if it appears that the E-Safety policy may have been breached, on the authorisation of the Designated Safeguarding Lead or the Head or, if it involves the Head, the Chair of Governors.

All staff

- Should acknowledge that they have read, understood and agreed with the E-Safety Staff Code of Practice, (see Appendix 1). They will know that by following the rules they are safeguarded

from allegations and that they understand their responsibilities to safeguard students when using on-line technologies.

They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

- When accessing the school system from home, the same Code of Practice will apply.

- Staff should request training or access internal training so that they are updated on new and emerging technologies and are up-to-date with E-Safety knowledge that is appropriate for the age group they teach and reinforce it through their curriculum.

- Ensure the correct procedure is used for dealing with any issues arising from indecent or pornographic/child abuse images sent/received (see Appendix 2).

- Ensure that students are protected and supported in their use of on-line technologies and are taught to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.

- To work closely with tutors and pastoral leaders regarding PSHE so that students are taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

- Staff are expected to be aware of and adhere to data protection rules when communicating by email and the age appropriateness and legalities of the resources they use and upload.

- They must report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies to the Deputy Head and, if necessary complete the appropriate logs of concern or discussion.

<u>Students' responsibilities</u>

- Students will fully participate in the E-Safety curriculum provided in ICT and PSHE lessons.

- Students are expected to use the Internet and other ICT e.g. mobile phones, digital cameras, webcams, in a safe and responsible manner at all times in school.

- Students are responsible for following the E-Safety code of conduct for students whilst within school.

- Students know that cyber bullying or posting of unauthorised content or malicious comments to or about other pupils or staff, is an extremely serious offence and the consequences would be enforced as per the Behaviour Management flowchart.

- Students should never bring the School into disrepute with regards to their digital use.

- Students are taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, and will be expected to do so knowing that they will not be reprimanded for behaviour which is not their responsibility.

Parents / carers

- All parents and carers have access to this policy via the School website.
- Parents / carers and students are asked to read the E-Safety code of practice to understand the implications for students if there should be any misuse of technologies.
- Are encouraged to seek advice and support from the school where necessary by contacting their child's Form Tutor, Head of Year or the Deputy Head

Inappropriate Use of IT

In the event of inappropriate use by Students:

When considering any sanction regarding the misuse of technology each case will be looked at individually and according to the levels of severity a range of sanctions will be considered.

Any student found to be misusing the Internet by not following the Acceptable Use Rules will have, as a minimum, a Day Book entry completed by the staff member observing the breach of the rules.

For more serious transgressions, parents/carers will be informed by letter outlining the breaches to the Code of Practice and any consequences such as removal of access to the internet. (see Appendix 2).

Following any further breaches parents/carers will be invited into school to discuss their child's online activity. We will see how we can support them through guidance and/or training. For example, we will refer to guidance from Child Exploitation and Online Protection (CEOP).

In the event that a student accidentally accesses inappropriate materials the student should report this to an adult immediately who should take appropriate action to hide the screen or close the window, and they should then refer the incident to the Network Manager who will ensure no further access to this site occurs through updating the filtering service. (see Appendix 2)

In the event of inappropriate use by Staff

If a member of staff is believed to misuse the Internet or E-learning platforms in an abusive or illegal manner, it will be reported to the Headmaster immediately. We will then follow our Discipline and/or Child Protection Policy as appropriate.

E-Safety in the curriculum

We will teach our students how to use the Internet safely and responsibly for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning. This will be done in all lessons using ICT and particularly through ICT and/or PSHE lessons so that the following concepts, skills and competencies are taught and revisited as needed. (For further details see PSHE schemes of work)

Use of E-mail

- The School has individual email addresses for students - used as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

    - Staff are only to use their School email addresses for communication between home and school. Students are encouraged only to use their school email to contact staff about issues relating to teaching and learning. Parents/carers are encouraged to be involved with the monitoring of e-mails sent although the best approach with students is to talk with them about who they may be communicating with, assessing risks together.

Filtering & Security System

- A filtering system is used which blocks listed sites and flags up concern in the usage of IT, for example accessing sites which may cause a concern according to the Prevent Strategy.

- Users should use only the school's Email system to communicate with each other. We can trace and recall all emails sent / received should it be required for further investigation. This will be conducted in conjunction with the Network Manager.

- Suspicious emails, including emails containing profanity, are quarantined and blocked if necessary.

- Any attempt to access a blocked URL is logged.

Mobiles and Smartphones

- The use of mobiles in school follows the school behaviour policy. Mobile phones may not be used in school except in Common Rooms for Years 9 and above or when instructed by a teacher in the context of education.

- Staff members are not allowed to use their personal telephones to contact students, except in emergency if on an off-site visit. They should not store students' numbers on their own phone – this includes students who have left the school in the last three years. If staff have any students' numbers held on personal telephones they must inform the Deputy Head of the numbers and the reason for holding them.

Photos & video

- Photographs and video images should only be recorded and / or uploaded on the approval of a member of staff or parent/carer and should not allow individual safety or privacy to be compromised (staff or student), it should only contain something that would also be acceptable in school. Parents/carers should monitor the content of photographs / videos uploaded at home.

- Group photographs are preferable to individual students and should not be of any compromising positions or in inappropriate clothing, e.g. swimming costumes.

- The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission must always be sought from the

parent/carer prior to the uploading of any images (this is done by electronic consent at the start of the year).

E-Safety Support & Advice

Links or feeds to E-Safety websites are provided on our website and new useful guides and links are posted on our front page to support our staff, students and parents in keeping safe online at home / via 3G. The CEOP (Child Exploitation and On-line Protection Centre) "Report Abuse" button is also available should there be a concern of inappropriate or malicious contact made by someone unknown. This provides a safe place for students to report an incident if they feel they cannot talk to a known adult. The CEOP button links to their website, www.thinkukknow.co.uk.

The E-Safety Code of Practice for staff and the E-Safety Policy are contained in the Staff Handbook as a reminder that staff members need to safeguard against potential risks. An E-Safety Guide for students will be displayed in ICT rooms to remind students of their need to safeguard themselves and others against potential harm from the internet.

E–SAFETY CODE OF PRACTICE FOR STAFF

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, we are asked to read, understand and apply this Code of Practice. This is so that we provide an example to students for the safe and responsible use of online technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

Personal responsibilities

- I will report any incidents of concern for children's or young people's safety or accidental misuse to the Headmaster, Designated Person for Child Protection or Network Manager in accordance with procedures listed in the E-Safety Policy.

- I know that images should not be inappropriate and should not reveal any personal information about children and young people.

For my protection as an adult working with young people

- I know that I should only use the school ICT equipment to carry out my professional school-related duties and I know that it is not advisable to store any personal details / files /photos etc. on school equipment.

- I will check with the ICT technical team before installing any hardware or software onto school equipment and ensure that appropriate licences are in place.

- I will only use my school email address to contact a student via their school email address.

- I will only use a personal mobile for emergency contact with parents or students and will inform the Deputy Head that I have done so.

- I will not store students' mobile numbers on my personal mobile and I am aware that this applies to numbers of students who have left the school in the last three years. If I hold these numbers in my phone I will inform the Deputy Head which numbers I hold.

- I will not communicate with current students via social media, for example adding them as friends on Facebook. I know that it is recommended practice that this also includes students who have been at the school in the last three years.

Security

- I know that I should complete or seek support to complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

- I will ensure that I keep my passwords secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password or I suspect that someone has used my password, I will report it immediately to the Network Manager.

- I understand that the necessary password length is a minimum of 8 characters and should include numbers as well as letters.

- I will generate a separate password for my School Base access as it holds very sensitive data.

- I have read and understood my responsibilities as outlined in the associated policies such as the child protection, appropriate conduct with students, behaviour and anti-bullying policies.

Student related professional duties

- I understand that I need to give permission to children and young people before they can use ICT
- equipment, smartphones etc., to capture images or upload images (video or photographs) to the Internet or send them via email.

- I will adhere to copyright and intellectual property rights.

I will agree that I have read, understood and agree with this Code of Practice on each logon to the School network.

Appendix II: Disciplinary Procedure for All School Based Staff

In the event that a member of staff may be seen to be in breach of behaviour and good conduct through misuse of on-line technologies, this policy outlines the correct procedures for ensuring staff achieve satisfactory standards of behaviour and comply with the rules of the Governing Body.

School Procedures Following Misuse by Staff

The Headmaster will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult employed by or working in the school:

A. An inappropriate website is accessed inadvertently:

Report website to the Deputy Head and the network manager who will ensure that it be added to the banned or restricted list.

B. An adult receives inappropriate material.

Do not forward this material to anyone else – doing so could be an illegal activity. Alert the Headmaster or Deputy Head immediately. Ensure the device is removed and log the nature of the material. Contact the relevant authorities for further advice e.g. police. Inform ICT technicians as in A.

C. An inappropriate website is accessed deliberately.

The person discovering this must:

Ensure that no one else can access the material.

Report to the Headmaster and Network Manager immediately. The Headmaster will refer back to the E-safety Policy and the E-Safety Staff code of practice and follow agreed actions for discipline. He will inform the ICT technical team to update the filtering service.

N.B. There are three incidences when we must report directly to the police.

1. Indecent images of children found.
2. Incidents of 'grooming' behaviour.
3. The sending of obscene materials to a child.

It is essential that in such instances that a member of the SLT is informed immediately on discovery.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine if they are unable to send out a forensics team immediately. If in doubt, do not power down the machine.

D. An adult has used ICT equipment inappropriately:

Follow the procedures for C.

E. An adult has communicated with a student inappropriately or used ICT equipment inappropriately.

The person discovering this must:

- Ensure the student is reassured and remove them from the situation immediately, if necessary.
- Report to the Headmaster and Designated Safeguarding Lead immediately, who should then follow the Child Protection Policy
- Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent.

Once Procedures and Policy have been followed and the incident is considered innocent, refer to the E-Safety Policy and E-Safety Staff code of practice.

If illegal or inappropriate misuse is known, contact the Headmaster or Chair of Governors (if the allegation is made against the Headmaster) and Designated Safeguarding Lead immediately and follow the Child Protection Policy. Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website or any other (or printed out) about a student or an adult in school:

- Preserve any evidence.
- Inform the Deputy Head immediately and follow Safeguarding Child Protection Policy as necessary.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Deputy Head or Headmaster.

Staff Procedures Following Misuse by Children and Young People

The Deputy Head will ensure that these procedures are followed, in the event of any misuse of the Internet, by a student:

A. An inappropriate website is accessed inadvertently:

Reassure the student that they are not to blame and praise for being safe and responsible by telling an adult. Report website to the network manager. The ICT Technician staff contact and update the filtering service locally so it can be added to the banned or restricted list.

B. An inappropriate website is accessed deliberately:

Refer the student to the Acceptable Use Rules. Reinforce the knowledge that it is illegal to access certain images and police can be informed. Decide on appropriate sanction. Notify the parent/carer.

C. An adult or student has communicated with a student or used ICT equipment inappropriately:

Ensure the student is reassured and remove them from the situation immediately. Report to the Designated Safeguarding Lead immediately. Preserve the information received by the student if possible and determine whether the information received is abusive, threatening or innocent. If illegal or inappropriate misuse the Headmaster or Deputy Head must follow the Child Protection Policy and contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website about a student in school:

Preserve any evidence. Inform the Headmaster immediately. Inform the Deputy Head and Network Manager so that new risks can be identified. Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about a student in the school:

Preserve any evidence. Inform the Deputy Head or Headmaster immediately. Follow Acceptable Use Procedures and Anti-bullying policies ensuring that all parents/carers of any students involved are informed of the incident and action taken.

Kirsten Pankhurst 26th October 2018. To be reviewed September 2019