BIRKENHEAD
SCHOOL

E-Safety Policy and Code of Practice

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 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 continue to be protected.

Aims

Birkenhead School aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention of grooming or exploiting them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of

nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Headmasters and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

Roles and responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headmaster to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Dr Julia Moore.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for all students, taking into account age, SEND and other relevant factors

The Headmaster

The Headmaster is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's DSL and Deputy DSLs are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headmaster in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headmaster, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headmaster and/or Governing Body

  This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as the Smoothwall filtering and monitoring system, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are flagged to the DSL and dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors, agency staff and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use

- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headmaster of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating students about online safety

Students will be taught about online safety as part of the curriculum including as part of Relationships and Sex Education (see separate policy). This can take place in ICT lessons, PSHE, Future Skills, Beyond the Curriculum and workshops delivered in-house or by external agencies:

In **Early Years** pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Students in **Junior Prep** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not

- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

In **Key Stage 3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via Firefly and as part of the Parent Seminar Programme. This policy will also be shared with parents.

Online safety could also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headmaster and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headmaster.

Cyber-Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the intentional harming of one person or group by another person or group, either one-off or repetitive, where the relationship involves an imbalance of power. (See also the anti-bullying policy)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors and teachers will discuss cyber-bullying with their tutor groups and this will be covered in assemblies and as part of the PSHE programme.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also provides information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the anti-bullying policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or

- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Students using mobile devices in school

The use of mobile phones in School is explained in more detail in the Mobile Phone Policy. Students using their mobile phones in School, where permitted, are bound by this policy.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – see advice on Firefly
- Not using mobile storage devices
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the network manager.

How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police and/or TRA.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on the DayBook. The use of the School network is monitored by Smoothwall and checked daily by the DSL.

This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the Governing Body.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- The Student and Staff Code of Conduct
- The Mobile Phone and BYOD Policy
- Data protection policy and privacy notices
- Complaints procedure
- Anti-bullying policy
- PSHE Policy
- Relationships and Sex Education Policy
- The internet acceptable use policies

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 two 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 two years, except for practical reasons for example networking on LinkedIn.

Security

- I know that I should use my School Laptop for working from home wherever possible. I will not carry data on removable devices.

- 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
- I will not use personal 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.