



THE Boswells SCHOOL

E-Safety Policy

A member of the Chelmsford Learning Partnership

Responsible	Local Governing Body
Lead Staff Member	Deputy Headteacher (Behaviour Welfare and Safety)
Approved by	Local Governing Body
Date Approved	3 rd December 2019
Version	2
Review Date	Autumn 2020

The Boswells School - E-Safety Policy

E-safety Policy Rationale:

E-safety encompasses Internet technologies and electronic communications such as laptops, tablets, mobile phones and wireless technology. It highlights the need to educate pupils about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Computing and ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of computing within our society as a whole. Currently the apps and software children and young people are using both inside and outside of the classroom include:

- Websites
- Podcasting
- Coding
- Gaming
- Mobile devices
- Video & Multimedia

Whilst exciting and beneficial all users need to be aware of the range of risks associated with the use of these technologies.

At The Boswells School we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of fixed and mobile internet technologies provided by the school. Any visitors using their own devices within school, adhere to the schools Acceptable Use Agreement and this e-safety policy.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-safety co-ordinators at The Boswells School is the Deputy Headteacher (Behaviour Welfare and Safety)

This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: computing, safeguarding, child protection, behaviour, health and safety, anti-bullying and Personal Development.

Managing the school e-safety messages

We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.

E-safety guidelines and the SMART rules will be prominently displayed around the school (see Appendix).

E-safety in the Curriculum

The school provides opportunities within a range of curriculum areas to teach about e-safety.

Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the e-safety curriculum.

The teaching of e-safety focuses on helping children to recognise inappropriate content, conduct, contact and commercialism and helps them learn how to respond or react appropriately.

Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues.

Pupils know how to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Managing the Internet

All internet activity within school is monitored and filtered. Whenever any inappropriate use is detected, the ICT Manager is notified and the incident will be followed up in line with the school Acceptable Use Policy.

The school maintains pupils will have supervised access to Internet resources (where reasonable) through the school's digital devices.

If Internet research is set for homework, staff will remind pupils of their e-safety training. Parents are encouraged to support and supervise any further research.

Infrastructure

Our internet access is monitored by IT system Administrators at The Boswells School and our ISP.

All domain joined devices connected to the IT infrastructure at The Boswells School are administrated by the IT system administrators.

Staff and pupils are aware that should they encounter or access anything unsuitable or damaging they must report it immediately to teachers, e-safety co-ordinator or the ICT Manager.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom.

The school is not responsible for the loss, damage or theft of any personal mobile device.

Pupils are not permitted to use mobile phones during the school day and mobile phones should not be seen at any point unless given express permission to use a school-approved app (e.g. Tassomai, PiXL).

Managing email

The use of email within school is an essential means of communication for staff.

Staff must use the school's approved email system for any school business.

Staff must inform (the e-safety co-ordinator/ line manager/ ICT Manager) if they receive an offensive or inappropriate e-mail.

Pupils:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which have a direct effect on the children's behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

All staff are aware of specific children in school who do or do not have photograph permissions. If they do have permission, staff are aware of the platforms they can be used on.

Staff are encouraged to use the School's own mobile devices and cameras, to record images of pupils, this includes field trips. If personal digital equipment, such as mobile phones are used, the images should be appropriate, upload to the school network or social media sites such as Twitter and then deleted immediately.

Publishing pupils' images and work

All parents/guardians will be asked upon entry to the school to give permission to use their child's work/photos in publicity materials or on the school website, twitter account or mobile app.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

Parents/carers may withdraw or amend permission, in writing, at any time.

Pupils' full names will not be published in association with their image and vice versa on the school website, twitter account, mobile app or any other school based publicity materials.

Storage of Images

Images/ films of children are stored securely on the school server and / or teacher's individual school laptops.

Misuse and Infringements

Complaints

Complaints or concerns relating to e-safety should be made to the e-safety coordinators, line manager or ICT Manager.

Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the teacher e-safety coordinators or ICT Manager.

Deliberate access to inappropriate materials by any user will lead to the incident being logged, in the first instance by the subject teacher and then forwarded to the e-safety co-ordinator. Depending on the seriousness of the offence, investigation maybe carried out by the Headteacher or LA. Staff are aware that negligent use or deliberate misconduct could lead to disciplinary action.

Equal Opportunities

Pupils with additional needs

The school endeavours to deliver a consistent message to parents and pupils with regard to the schools' e-safety rules.

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues; careful consideration is given to group interactions when raising awareness of e-safety.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school website. This policy underlines the school role in ensuring its community is safe and every reasonable steps will be taken to ensure this is the case. However technology may outstrip some of the issues and practicalities discussed here hence the policy will be reviewed on a yearly cycle.

Appendix:

1) SMART poster

S **SAFE** Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online. 

M **MEETING** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. 

A **ACCEPTING** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages! 

R **RELIABLE** Information you find on the internet may not be true, or someone online may be lying about who they are. 

T **TELL** Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. 
You can report online abuse to the police at www.thinkuknow.co.uk 

080172