E-Safety Policy

Prepared By	Chris James-Roll Head Teacher
Approved by the Proprietor	Keith Boulter
Date Approved	September 2025
To Be Reviewed	September 2026

E-Safety Policy

Introduction

As part of the Education Act and the Children's Act, it is the duty of schools to ensure that children are protected from potential harm both within and beyond the school 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 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 about the pros and cons of using new technologies both within and outside School.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the School.
- 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 and Responsibilities of the School

Head Teacher and Responsibilities

- It is the overall responsibility of the Head Teacher to ensure that there is an overview of e-Safety as part of the wider remit of safeguarding across the school with further responsibilities as follows:
- The Head Teacher is the designated e-Safety Lead and will implement agreed policies, procedures, staff training, curriculum requirements and to take responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- Time and resources is provided for the e-Safety Lead and staff to be trained and update policies, where appropriate.
- The Head Teacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the School Improvement Plan.
- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures, and appropriate action is taken, even to the extreme of suspending a member of staff, informing the police (via establishment's agreed protocols with the police) or involving parents/carers.

The e-Safety Lead

It is the role of the designated e-Safety Lead to:

- Challenge the School about having:
    - Firewalls.
    - Anti-virus and anti-spyware software.
    - Filters.
    - Using an accredited ISP (internet Service Provider).
    - Awareness of wireless technology issues.
    - A clear policy on using personal devices.

    - Personal devise use in school (students and staff).

- Appreciate the importance of e-safety within School and to recognise that all educational establishments have a general duty of care to ensure the safety of their students and staff.
- Establish and maintain a safe ICT learning environment within the School.
- Ensure that the Policy is reviewed annually, with up-to-date information, and that training is available for all staff including care staff.
- Ensure that filtering is set to the correct level for staff and children in the initial set-up of a network, stand-a-lone PC, staff/children laptops and the learning platform *or ensure the technician is informed and carries out work as directed*.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children.
- Report issues to the Proprietor at least annually and when need arises. To make sure that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- One to one support to ensure monitoring of students use of the Internet and online technologies.
- Log of incidents as safeguarding incidents, where risks are identified.
- To ensure there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.
- Ensure that unsolicited e-mails to a member of staff from other sources is minimised. Refer to the Managing Allegations Procedure, SSCB, for dealing with any issues arising from indecent or pornographic/child abuse images sent/received.
- Ensure there is regular monitoring of internal e-mails, to ensure that the tone of e-mails is in keeping with all other methods of communication.
- Report overuse of blanket e-mails or inappropriate tones to the Head Teacher.

Staff or Adults

It is the responsibility of all adults within the School to safeguard children from harm:

- Be familiar with the Behaviour, Anti-Bullying and other relevant policies and report concerns.
- Check the filtering levels are appropriate for their children and are set at the correct level. Report any concerns.
- Alert the e-Safety Lead about any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children are protected and supported in their use of technologies so that they know how to use them in a safe and responsible manner.
- Be up-to-date with e-Safety knowledge that is appropriate for the age-group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998. Remember confidentiality and know not to disclose information from the network, pass on security passwords or leave a station unattended when they, or another, user is logged in.
- Ensure that School follows the correct procedures for any data required to be taken from the School premises.
- Report accidental access to inappropriate materials to the e-Safety Lead in order that inappropriate sites are added to the restricted list or filter.

- Use anti-virus software and check for viruses on their work laptop or memory stick when transferring information from the internet on a regular basis, especially when not connected to the School's network.
- Ensure that all personal storage devices (i.e. memory sticks) which are utilised by staff members to hold sensitive information, are encrypted or password-protected in the event of loss or theft.
- Report incidents of personally-directed "bullying" or other inappropriate behaviour via the Internet or other technologies to the SDP.

Children
Should be:

- Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand.

Appropriate and inappropriate Use by Staff or Adults
Staff members have access to the network so that they can obtain age-appropriate resources for their classes and create folders for saving and managing resources. 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. Staff all receive a copy of the 'Code of Conduct Policy' and 'ICT & Internet acceptable use policy' which they are required to read and understand as part of the induction process.

In the Event of Inappropriate Use by Staff
If a member of staff is believed to misuse the internet or learning platform in an abusive or illegal manner, a report must be made to the Head Teacher immediately and then the Managing Allegations Procedure and the Safeguarding Policy must be followed to deal with any misconduct and all appropriate authorities contacted. In the lesser event of misuse or accidental misuse, this should be referred to the Head Teacher and noted.

It is also intended to provide support and information to parents when children may be using the Internet outside School. It is hoped that parents / carers will inform School of any potential issues that they feel should be addressed, as appropriate.

File-sharing via e-mail, weblogs, the downloading of materials, for example, music files and photographs, need to be appropriate and 'fit for purpose' based on research for work and be copyright-free.

Action In the Event of Inappropriate Use
Should a child or young person be found to misuse the online facilities whilst at School, the following consequences should occur

- Any child found to be misusing the internet will be sanctioned appropriately
- Further misuse may result in not being allowed to access the internet for a period of time.
- A notice will be sent to carers/social workers outlining the breach in Safeguarding Policy where a child or young person is deemed to have misused technology against another child or adult. The Head Teacher will also take appropriate disciplinary action.

In the event that a child or young person accidentally accesses inappropriate materials, the child should report this to an adult immediately and take action to hide the screen or close the window without deleting it, so that an adult can take the appropriate action to filter the site.

Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can access public report systems including (www.thinkuknow.co.uk) to make a report and seek further advice. A display in school provides information about how to make a report and PSHE lessons remind students.

Deliberately misusing online technologies will be taken very seriously indeed by the School, parents and social works will always be contacted.

Children should be taught and encouraged to consider the implications of misusing the internet and posting inappropriate materials to websites - for example, this may have legal implications.

The Curriculum and Tools for Learning

Internet Use

School will teach children how to use the Internet safely and responsibly. They should also be taught, through ICT/Computing and/or PSHE lessons, how to research information, explore concepts and communicate effectively in order to further learning. The following concepts, skills and competencies should have been taught by the time they leave:

- Internet literacy.
- Making good judgements about websites, APPs and e-mails received.
- Knowledge of risks such as viruses and opening mail from a stranger.
- Access to resources that outline how to be safe and responsible when using any online technologies.
- Knowledge of copyright and plagiarism issues.
- Knowledge of inappropriate file sharing and downloading illegal content and its consequences.
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.

These skills and competencies are taught within the curriculum so that children have the security to explore how online technologies can be used effectively but in a safe and responsible manner. Children should know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture in the event that they have accidentally accessed something.

For personal safety, we ensure information uploaded to web sites does not include any personal information such as:

- Full name (first name is acceptable, without a photograph).
- Address.
- Telephone number.
- E-mail address.
- Age or DOB.
- Names of parents.
- Routes to and from School.
- Identifying information, e.g. I am number 8 in the School Rugby Team.

Photographs of children in School or on Out and Abouts or external activities should only contain something which would also be acceptable in 'real life'. Images of children should be taken only with the School camera and stored only on the secure school one drive photos folder, where they can be printed from. Parents / Carers taking photographs on sports days, at plays and concerts should be made aware of the School policy on recorded images and they should never be shared in the public domain. Only children whose parents, carers or social workers have signed the Photo

Permission form, maybe photographed. A log of these permissions is held in the main school office.

Social Media
Staff or adults need to ensure they consider the risks and consequences of anything they or their children may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

It is illegal in the UK to have a Facebook presence before the age of 13. The School filter excludes Facebook and other known social media sites. However, if children are provided with 3G or 4G devices, we cannot ensure that children are using the internet safely and appropriately. **Broadlands Hall School students are not permitted to use their phones or personal tablets in school at any time**.

Carers, in conjunction with school staff, must ensure that their children's privacy settings are appropriate and that personal details or anything that will put a child (Under 18s) at risk is not posted online. Once a video / photograph / comment is posted, it is near impossible to remove and it will be there for life.

Children should be advised on social networking security and recommendations made for privacy settings to be activated to 'Friends only' for all applications to restrict unsolicited access. The importance of passwords and blocking unwanted communications is also highlighted.

Adults should be aware that social networking can be a vehicle for cyber-bullying. Students are encouraged to report any incidents of bullying to the School, allowing for the procedures, as set out in the Anti-Bullying Policy, to be followed.

School Website
The uploading of images of students to the School website must be agreed with the Head Teacher and adults with parental responsibility must give their permission. The School will consider which information is relevant to share with the general public on a website.

External Websites
In the event that a member of staff finds himself or herself or another adult on an external website, such as 'Rate My Teacher', as a victim, this must be reported to the Head teacher and the School will report incidents to Social Services or the Police.

Mobile Phones and Other Emerging Technologies
However, given the vulnerability of our students we have, for the time being, concluded that it is in the interests of safety for all to have a total ban on student phones and personal devises in school.

- *Inappropriate or bullying text messages.*
- *Images or video taken of adults or peers without permission being sought.*
- *'Happy slapping' – the videoing of violent or abusive acts towards a child, young person or adult.*
- *Sexting - the sending of suggestive or sexually explicit (not necessarily involving nudity) personal images via mobile phones.*

Students at Broadlands are not allowed to use mobile phones or other personal technology during the school day.

Personal Mobile Devices for Staff
Staff are allowed to bring in personal mobile phones or devices for their own use but **must not use personal numbers to contact children under any circumstances. Staff are not allowed to use their phones during the school day, unless in an emergency away from students**

- Staff must ensure that there is no inappropriate or illegal content stored on the device and should be aware that using features, such as video or sound recording, may be subject to the same procedures as taking images from digital or video cameras.
- Staff should be aware that games consoles such as the Sony Playstation, Microsoft Xbox, Nintendo Wii and DSi and other such systems have Internet access which may not include filtering. Before use within School, authorisation should be sought from the Head teacher and the activity supervised by a member of staff at all times.
- The School is not responsible for any theft, loss or damage of any personal mobile device.
- Staff phones should not be used in front of students at any time except strictly on school business/in an emergency.

School-Issued Mobile Devices
The management of the use of these devices is similar to those stated above, but with the following addition:

- Where School has provided a mobile device to a member of staff, such as a laptop, PDA or mobile phone, only this equipment should be used to conduct School business.

Video and Photographs
The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone.

When in School there is access to:

- Stills Cameras (kept in the Main Office)

The sharing of student photographs via weblogs, forums or any other means online is forbidden.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a School website. Photographs should only ever include the child's initial.

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing.

It is current practice not to permit external media such as local and national newspapers to include the names of our student in their publications. Photographs of children/young people should only be used after permission has been given by the Head teacher plus parent/carer.

Video-Conferencing and Webcams

Publicly accessible webcams are not used in School.

Taking images via a webcam is not permitted.

Permission should be sought from parents and carers if their child is engaged in video-conferencing with individuals or groups outside the School. This process should always supervised by a member of staff and a record of dates, times and participants held by the School.

Children need to tell an adult immediately of any inappropriate use by another child or adult.

Social Networking Advice for Staff
Social networking outside of work hours, on non-School-issued equipment, is the personal choice of all School staff. Owing to the public nature of such websites, it is advisable for staff to consider the possible implications of participation. The following advice should be considered if involved in social networking:

- Personal details are never shared with students such as private email address, telephone number or home address. Staff must ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles. The simplest and most effective way to do this is to remove details from search results and turn off public visibility.
- Staff should not engage in personal online contact with students outside of Head teacher-authorised systems.
- Staff should ensure that full privacy settings are in place to prevent students from accessing photo albums or personal information.
- Staff are advised against accepting invitations from colleagues until they have checked with them in person that the invitation is genuine (avoiding fake profiles set up by students).

Security
Anti-virus and anti-spyware software is used on all network and standalone PCs or laptops and is updated on a regular basis.

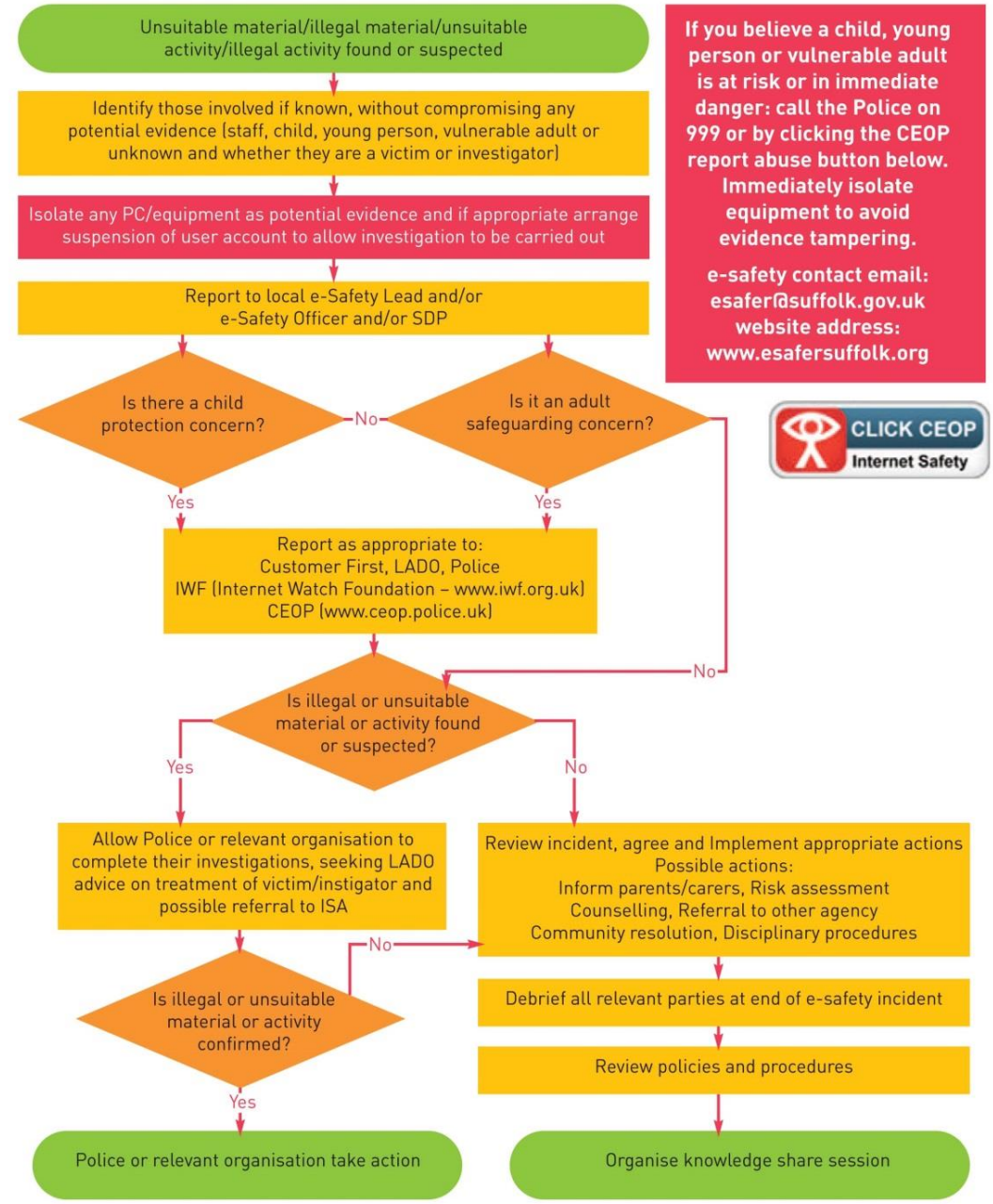
All social networking sites such as Facebook and Instagram are blocked by the school ICT filter. Staff can access YouTube.

A firewall ensures information about children and the School cannot be accessed by unauthorised users. In addition, the data on the school server requires login to access it.

Monitoring
The e-Safety Lead and all staff will monitor the use of online technologies by children on a regular basis. The school uses ITEX for all ICT related enquiries, support and managing the system.

Support for, and support from, carers
As a part of Broadlands Hall commitment to developing e-safety awareness with children, the School may offer carers the opportunity to find out more about how they can support the School in keeping their child safe on line and to find out what they can do to continue to keep them safe whilst using online technologies beyond School. We aim to promote a positive attitude to using the World Wide Web and, therefore, want carers to support their child's learning and understanding of how to use online technologies safely and responsibly.

Curriculum Development
The teaching and learning of e-Safety is embedded within the School curriculum to ensure that the key safety messages about engaging with people are the same whether children are on or off line. It forms part of the PSHE programme but is not exclusive to this area of curriculum and opportunities to embed e-Safety throughout the curriculum are widespread.

Fig 1: e-Safety Flow Chart

e-Safety Incident Flowchart