THE SOUTHOVER PARTNERSHIP
TRUST - BELIEVE - SUCCEED

Online Safety Policy

Date adopted	October 2023
Date of last Review	August 2023
Next review due:	August 2024 and in line with DFE updates

Rationale

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

- However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:
- Access to illegal, harmful or inappropriate images or other content
- Un-authorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Filtering and Monitoring

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.   Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions. The designated safeguarding lead has the responsibility for understanding the filtering and monitoring systems and processes. While the proprietor body (Board of Trustees) have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met, the Executive Headteacher – Kief Ho, and Safeguarding Link Trustees - Lynn Yap and Katie Adams, ensure the digital and technology standards are met.

- The senior leadership team are responsible for:
- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of provision
- overseeing reports
- making sure that all staff understand their role
- making sure that all staff are appropriately trained
- making sure that all staff follow policies, processes and procedures
- making sure that all staff act on reports and concerns

The Southover partnership uses a filtering and monitoring system to keep all networker users (including those who use a school device and network) from accessing any inappropriate contents including but not limited to: fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, harmful online interaction with other users, online behaviour that increases the likelihood of, or causes, harm, risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Staff must report to a safeguarding lead should they suspect a network user of accessing inappropriate contents.

The filtering and monitoring protocol

A weekly log on filtered materials (identified by users and user groups) is produced to the designated safeguarding lead for review with details including when the checks took place, the person(s) who completed and what was filtered. In addition to the regular reports, the designated safeguarding lead will also be notified immediately when anything is filtered and flagged up. The filtering and monitoring protocol applies to school owned devices and services, geographical areas across the sites.

Contents that required filtering include, but not limited to: fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, harmful online interaction with other users, online behaviour that increases the likelihood of, or causes, harm, risks such as online gambling, inappropriate advertising, phishing

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems
- The IT service provider should have technical responsibility for:
- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems
- The IT service provider should work with the senior leadership team and DSL to:
- procure systems
- identify risk
- carry out reviews
- carry out checks

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors) who have access to and are users of school IT systems, both in and out of school.

The Education and Inspections Act 2006 empowers the Executive Headteacher, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti- bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Roles and Responsibilities

Board of Trustees

The Trustees are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness.

- **Executive Headteacher / Senior Leaders**
- The Executive Headteacher is responsible for ensuring the online safety of the school, though the day-to-day responsibility for online safety will be delegated to the Deputy designated Safeguarding Lead.
- The Executive Headteacher is responsible for the implementation and effectiveness of this policy. They are also responsible for reporting to the Trustees on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Executive Headteacher / SLT are responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles.
- The Executive Headteacher / SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Executive Headteacher and another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Designated Safeguarding Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Reports to the School Leadership Team serious breaches of the Online Safety Policies
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Are trained in and shares with staff an awareness and understanding of online safety issues and the potential for serious child protection issues that can arise from:
  - Sharing of personal data
  - Access to illegal / inappropriate materials
  - Inappropriate on-line contact with adults / strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying
  - Sexting
  - Revenge pornography
  - Radicalisation (extreme views)
  - CSE

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the Online Safety policy, school Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Designated Safeguarding Lead for investigation/action/sanction
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level
- Students / pupils understand and follow, as appropriate for age and ability, the school online safety and acceptable use policy
- Students / pupils understand and follow Online safety rules and they know that if

these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies.

- In lessons where internet use is planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Pupils

- Are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be expected to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc.
- Should understand that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school, where appropriate for age and ability.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through review meetings, letters, website / local online safety campaigns / literature. Parents and carers will be responsible for:

- Endorsing (by signature) the Student / Pupil Acceptable Use Agreement
- Accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy.

Parents / carers should understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

The Southover Partnership ensures that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement. However, the breadth of issues classified within online safety is considerable and ever evolving but can be

categorised into four areas of risk:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, 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

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

It is essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. In addition to the annual safeguarding training, staff also receive termly safeguarding quizzes.

Education and Training

Education – Pupils

Online safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned online safety programme should be provided as part of Computing / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students / pupils should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils are taught the importance of keeping information such as their password safe and secure.

- Rules for the use of ICT systems / internet will be made available for pupils to read
- Staff should act as good role models in their use of ICT, the internet and mobile devices
- Students / pupils are taught how to keep safe though effective / good Online safety practice as part of an integral element of the school Computing curriculum and within their ICT learning.
- Where students / pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT and Facilities Officer (and other relevant person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need

Education – Parents and Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report). The school will therefore seek to provide information and awareness to parents and carers through regular online safety updates.

Education and Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school online safety policy and Acceptable Use Policies
- The Online safety Coordinator (or other nominated person) will provide advice/ guidance/training to individuals as required

Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images should only be taken on school equipment. The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Written permission from parents or carers will be obtained before photographs of students/pupils together with their name are displayed on school displays, in newsletters and in their child's own and other children's learning journeys.
- Written permission from parents or carers will be obtained before photographs of students/pupils together with their name displayed alongside are published in leaflets, posters, documents, training materials or used by the press.
- Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website or social media. Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the Data Protection Policy.

Communications

When using communication technologies, the school considers the following as good practice:

- Users need to be aware that email communications may be monitored.
- Users must immediately report to the Designated Safeguarding Lead – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be placed on the school website on public facing calendars and only official school emails should be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. Under no circumstances should a member of staff use their personal devices including mobile phones, to contact a pupil, parent/carer.

Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The incident should be following in accordance with the safeguarding policy and if necessary, the police should also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

Monitoring and review

This policy will be reviewed annually, or earlier, if necessary, in line with national and/or local updates.

Guidelines for the use of communication technologies within school

	Staff & other adults				Students / Pupils			
	Allowed	Allowed in designated areas/times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought to school	✓							To be handed in at start of day
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓						✓
Taking photos on mobile phones or personal camera devices				✓				✓
Use of personal handheld devices		✓						✓
Use of personal email addresses in school, or on school network during own time				✓				✓
Use of school email for personal emails				✓				✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites				✓				✓
Use of personal blogs				✓				✓
Use of educational blogs	✓						✓	