Brook Learning Trust
E-safety and Information Systems: Acceptable Use Policy

Introduction
At Brook Learning Trust we bring together our unique academies in our belief in the power of education to change lives and communities. It is our steadfast purpose to challenge and defy the barriers that constrain the educational progress of any child. We set high aims for aspiration and secure collective responsibility for all our children's achievements. Our work is underpinned by the values of Integrity, Respect, Courage, Optimism, Excellence and Accountability.

1. Policy Aims and Scope

This online safety policy has been written by Brook Learning Trust, building on the Kent County Council/The Education People online safety policy template. It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' 2018, 'Working Together to Safeguard Children' 2018, the Teaching Standards, Children Act 2004, section 11, Data Protection Legislation, including General Data Protection Regulations (GDPR) and Data Protection Act 2018 and the Kent Safeguarding Children Board procedures.

Purpose
The purpose of this policy is to:
- Safeguard and protect all members of the Trust and academy communities online
- Encourage all community members to develop responsibility for their behaviour and practice online
- Outline to staff and learners acceptable and unacceptable behaviours and the sanctions for unacceptable use
- Identify what monitoring takes place on ICT systems on site, or via devices provided by the Trust
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns
- Identify clear procedures to use when unacceptable use is suspected or identified.

The Trust identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

Policy Scope
The Trust believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The Trust identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life
- The Trust believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online
- This policy applies to all staff including those in a governance role, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the Trust and its academies (collectively referred to as "staff" in this policy) as well as learners, parents and carers

- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with Trust issued devices for use off-site, such as a work laptops, tablets or mobile phones
- This policy should be read in conjunction with the Staff Code of Conduct, Staff Disciplinary and Conduct Matters Policy and Procedure, Allegations of Abuse against Staff Policy, Behaviour Policy, Safeguarding Policy, Data Protection Policy and Sex, Preventing Extremism and Radicalisation Policy and Relationship Education Policy.

2. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) (see **Appendix Five** for details) has lead responsibility for online safety. The Trust and academies recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

Trustees / Academy Councillors

- The Audit & Risk Committee is responsible for ratifying this document bi-annually
- One or more Academy Councillors have responsibility for monitoring safeguarding in each academy and will make a minimum of three visits per annum to meet with the Designated Safeguarding Lead (DSL)
- Safeguarding Councillors' reports are submitted to the Audit & Risk Committee which meets three times a year and reports any concerns to the Trust Board.

Principal and Members of the Senior Leadership Team (SLT)

- The Principal has a duty of care for ensuring the safety (including e-safety) of all members of the academy community, though the day-to-day responsibility for e-safety will be delegated
- The Principal and/or SLT will invoke the BLT Staff Disciplinary and Conduct Matters Policy and Procedure in the event of a serious e-safety allegation being made against a member of staff
- The Principal will ensure that academy staff receive appropriate training in e-safety and related matters
- The Principal will ensure that the DSL with responsibility for e-safety is supported to undertake their roles; their performance will be monitored
- The Principal will ensure that e-safety is intrinsic to all areas of the curriculum and academy activities
- The Principal will review and ensure compliance with this policy and procedures
- The Principal will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety breach.

Network Manager/ICT Support Staff

- Will undertake regular monitoring of the information systems: both hardware and software
- Will ensure that Trust information systems comply with statutory e-safety technical requirements and adopt best practice
- Will ensure that the Trust technological and electronic infrastructures are secure and not open to misuse or malicious attack
- Will ensure that users of Trust information systems may only access the networks and devices by way of protected and regularly changed passwords
- Will ensure that staff and students are denied access to inappropriate websites and digital material from Trust information systems
- Will monitor the application, and oversee updates, of the internet filtering policy (more than one person will be involved with this)
- Will ensure that their CPD is kept up to date.

Teaching and Support Staff

- Are expected to be aware of e-safety related Trust and academy policies
- Must read, understand and sign the E-Safety and Information Systems: Acceptable Use Policy Acknowledgement – Staff form (**Appendix One**) before they are granted access to the information systems
- Will report any suspected misuse of the information systems to the Principal

- Will conduct all digital communications with students/parents/carers and others in a professional manner
- Will only communicate with parents/carers and students via Trust information systems
- Must ensure that students understand and abide by the terms of this E-safety Information Systems: Acceptable Use Policy
- Will instruct students in research skills, the avoidance of plagiarism and an awareness of copyright
- Will oversee the use of all digital devices and systems on Trust premises and ensure compliance with all relevant policies.

Designated Safeguarding Leads (DSLs)
- Will be trained in their roles to protect students and staff from breaches of e-safety
- Will ensure that staff and students:
  - Refrain from sharing personal data and/or digital images
  - Are denied access to inappropriate websites and digital material from Trust information systems
  - Understand the danger of establishing online contact with strangers via social networking or similar platform
  - Are aware of the dangers of grooming
  - Feel able to report incidents of cyber-bullying and/or breaches of e-safety.

Students
- Must read, understand and adhere to the terms of the E-Safety and Information Systems: Acceptable Use Policy – Parents/Carers and Students (**Appendix Two**) (including use of personal mobile phones and tablets)
- Will be instructed in research skills, the need to avoid plagiarism and the importance of complying with copyright regulations
- Will know the procedures for reporting incidents of abuse, misuse of the information system or access to inappropriate material
- Will be instructed in the importance of adopting good e-safety practices in and out of school.

Parents / Carers
- Parents/carers play a crucial role in ensuring that their children understand the need to access online material and information with care and in an appropriate way. Each academy will assist parents to understand e-safety related issues.
- Parents must read this policy and sign the E-Safety and Information Systems: Acceptable Use Policy Acknowledgement - Parent/Carer and Students form (see **Appendix Two**) before their child is granted access to the Trust system.

Visitors/Volunteers
- Visitors/volunteers who require temporary access to our IT network will be asked to sign the Visitor/Volunteer Information Systems: Acceptable Use Policy (**Appendix Three**) before being granted access to a Trust information system
- Visitors/volunteers who do not require access to our IT network but who use our Wi-Fi will be required to sign the Visitor/Volunteer Wi-Fi Acceptable Use Policy (**Appendix Four**).

3. Education and Engagement Approaches

Education and Engagement with Learners

The academy will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE). This is delivered through discreet PSHE lessons and where appropriate special events
- Reinforcing online safety messages whenever technology or the internet is in use
- Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation

- Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Displaying acceptable use posters in all rooms where students can access the internet
- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches
- Ensure all learners read this policy and sign the E-Safety and Information Systems: Acceptable Use Policy Acknowledgement – Parents/Carers and Students form (**Appendix Two**).

Vulnerable Learners

- The academy recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss
- The academy will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.

Training and Engagement with Staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with annual updates and regular briefings through the year
- This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices
- Make staff aware that their online conduct outside of the academy, including personal use of social media, could have an impact on their professional role and reputation
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community
- Ensure all members of staff read this policy and sign the E-Safety and Information Systems: Acceptable Use Policy Acknowledgement - Staff form (**Appendix One**).

Awareness and Engagement with Parents and Carers

- The academy recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies
- We will build a partnership approach to online safety with parents and carers by:
  - Providing information and guidance on online safety in a variety of formats
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as at parent evenings.
  - Drawing their attention to this policy and expectations in newsletters, letters, our prospectus and on our website
  - Requiring them to read this policy and discuss the implications with their children.

4. Reducing Online Risks

The academy recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

- We will:
  - Regularly review the methods used to identify, assess and minimise online risks
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
  - Recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices

- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

Classroom Use

- The academy uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Digital cameras, web cams and video cameras
  - SIMS.
- All Trust owned devices will be used in accordance with this policy and with appropriate safety and security measures in place
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information
- Supervision of learners will be appropriate to their age and ability
- We will balance children's ability to take part in age appropriate peer activities online, with the need to detect and prevent abuse, bullying or unsafe practice by children.

Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems
- All staff, learners, volunteers and visitors will read and sign an appropriate acceptable use policy acknowledgement form (**Appendices One, Two, Three and Four**) before being given access to our computer system, IT resources or internet.

Filtering and Monitoring

- Academy Leaders and Academy Councillors have ensured that our academies have age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, made with consent from the leadership team; all changes to the filtering policy are logged and recorded
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential
- Our academies use EIS Kent County Council (The Ebbsfleet Academy) and Smoothwall web filtering (The Hayesbrook School and The High Weald Academy) which block sites which can be categorised as pornography, racial hatred, extremism, gaming and sites of an illegal nature
- These filtering system blocks all sites on the Internet Watch Foundation (IWF) list
- We work with these organisations named above and Lightspeed Rocket to ensure that our filtering policy is continually reviewed
- If learners discover unsuitable sites, they will be required to:
  - Report the concern immediate to a member of staff
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

Monitoring

- We will appropriately monitor internet use on all Trust owned or provided internet enabled devices. This is achieved by using the impero service which is enabled on all machines and devices in the building
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation
- Staff, visitors, volunteers and learners must not try to bypass the filtering system.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred, deleted and made available online in accordance with General Data Protection Regulations and Data Protection legislation.

Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly
  - Encryption for personal data sent over the internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
  - Not using portable media without specific permission; portable media must be encrypted and will be checked by an anti-virus /malware scan before use
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments
  - Regularly checking files held on our network
  - All users are expected to log off or lock their screens/devices if systems are unattended.

Password Policy

All members of the academy will have their own unique username and private passwords to access our systems; all are responsible for keeping their password private.

- We require all users to:
  - Use strong passwords for access into our system
  - Always keep their password private; users must not share it with others or leave it where others can find it
  - Not to login as another user at any time.

Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the DfE
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright
- Staff or learner's personal information will not be published on our website; the contact details on the website will be an academy address, email and telephone number
- The administrator account for our website will be secured with an appropriately strong password
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community
- We will ensure that all images and videos shared online are used in accordance with the associated polices, including: E-safety and Information Systems: Acceptable Use policy, Data Protection policy, Safeguarding policy, Preventing Extremism and Radicalisation and Staff Code of Conduct.

Social Media

The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger. All members of the Trust community are expected to engage in any social media in a positive, safe and responsible manner.

Staff expectations

- All members of the Trust community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others

- Concerns regarding the online conduct of any member of the Trust community on social media should be reported to the DSL and will be managed in accordance with policies listed in section 1.
- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Staff Code of Conduct and Safeguarding policy
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites
  - Being aware of location sharing services
  - Opting out of public listings on social networking sites
  - Logging out of accounts after use
  - Keeping passwords safe and confidential
  - Ensuring staff do not represent their personal views as that of the Trust.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites
- Members of staff will notify a member of the Senior Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with Learners and Parents and Carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles
- Any pre-existing relationships or exceptions that may compromise this will be discussed with DSL or Principal
- Staff will not use personal social media accounts to contact learners or parents
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including the Behaviour Policy
- Learners will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
  - To only approve and invite known friends on social media sites and to deny access to others by making profiles private
  - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
  - To use safe passwords
  - To use social media sites which are appropriate for their age and abilities
  - How to block and report unwanted communications
  - How to report concerns both within the Trust and externally.

Official Use of Social Media

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Principal

- Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only
- Official social media use will be conducted in line with existing policies, including those listed in section 1
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.

Email

- Users are responsible for all email sent and for contacts established which may result in email being received
- Email should be worded in a manner appropriate for a professional educational institution, particularly as messages may be forwarded, inadvertently sent to the wrong person, printed and otherwise seen by unintended recipients. Emails containing personal information may also be disclosed as part of Subject Access Request made under the Data Protection Act 2018
- Students who receive offensive email must immediately tell a staff member
- Staff who receive offensive email must immediately tell a member of SLT or the Trust Executive
- Email should be used for Trust and academy purposes only
- Personal use of the email system is forbidden. Trust and academy email addresses may not be used for signing up to social networking/media sites, shopping sites, personal banking or other sites unrelated to the Trust
- Personal emailing or messaging between staff and students is not permitted
- Email should not be sent or forwarded to personal accounts outside the Trust's systems
- Email communications between staff and students: messages must be restricted to Trust/academy email addresses
- Students must not reveal personal details of themselves or others in email communications and must never use the system to arrange to meet anyone unknown to their families
- Emails sent to parents and to external agencies in furtherance of Trust activities may only be sent using a Trust/academy email account; messages should be worded appropriately, using the same stylistic conventions as a letter written on Trust or academy headed paper
- The forwarding of chain letters/emails via Trust/academy email addresses is not permitted
- Staff/Student photographs are displayed in the email address books of all Trust/academy users, to assist identification. These photographs are only visible by users inside the Trust/academy email systems
- Trust/academy email accounts must not be accessed via third-party applications
- Trust/academy email accounts may be only be stored on personal devices such as laptops and smartphones with the prior agreement of the IT Network Manager. Where access is agreed, devices must be encrypted and have a passcode/password
- If email is accessed on a personal device, message notifications should be restricted so that the content of emails are hidden on the device home/lock screen
- In the event that a device to which Trust/academy data have been downloaded is lost or compromised, the Network Manager reserves the right to erase the device remotely
- Users should be aware that email communications are monitored; the Trust reserves the right to access Trust/academy email accounts at any time.

External Hosted Services

The Trust/academies may use external companies to provide extra services to staff/student/parents; these could include:

- Learning materials
- Homework Systems
- Virtual Learning Environment (VLE)
- Parents Evening Systems
- Reporting Systems
- Communications systems
- Payment Systems.

Account and password details associated with these systems should not be made available to any other person.

Remote Access

- Remote access is provided to allow users access to Trust/academy software. Remote access is provided in order that users can access data stored on the system and thus to avoid the transfer of data to personal devices off site
- Remote access is provided to facilitate access to management and other sensitive data which must remain on the system and not be transferred to personal devices
- Remote access via public computers and from public locations, i.e. libraries, cafés etc. is discouraged given the confidential nature of the information available through SIMS and other systems
- Copying software and/or data from the remote server is not permitted.

Personal Mobile Phones and Tablets

- Use of personal mobile phones and tablets is governed by the relevant academy
- Staff are not permitted to use their personal mobile phones or tablets for contacting students or their families in their professional capacity
- Staff and visitors are not permitted to use personal mobile phones or devices to take photos or video footage of students: only devices owned by the Trust should be used for these purposes for professional purposes by Trust employees only
- Staff must not keep school related data or images on personal devices.

5. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns
  - Learners, parents and staff will be informed of our Complaints Procedure policy and staff will be made aware of the Whistleblowing Policy.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice from the Kent Education Safeguarding Team. Contact details and other areas of support can be found at **Appendix Five**
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or Principal will speak with Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised

Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns
  - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Board thresholds and procedures
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the Principal, in accordance with the appropriate policy, as listed in section 1
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer)
- Appropriate action will be taken in accordance with our Staff Disciplinary and Conduct Matters Policy and Procedure, Allegations of Abuse against Staff Policy and the Staff Code of Conduct.

6. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- The Trust has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- The Trust recognises that sexual violence and sexual harassment between children can take place online. Examples may include: non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation
  - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our safeguarding and behaviour policies.
- The Trust recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities
- The Trust also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online
- The Trust will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment
- If made aware of online sexual violence and sexual harassment, we will:
  - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies
  - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice
  - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
  - Implement appropriate sanctions in accordance with our behaviour policy
  - Inform parents and carers, if appropriate, about the incident and how it is being managed
  - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police
  - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
  - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Youth Produced Sexual Imagery ("Sexting")

- The Trust recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy)

- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery"
- The Trust will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using Trust provided or personal equipment
- We will not:
  - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so
    - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
  - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures
  - Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
  - Store the device securely
  - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image
  - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies
  - Inform parents and carers, if appropriate, about the incident and how it is being managed
  - Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
  - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible
  - Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
  - Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Trust will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns
- The Trust recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy)
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally

- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
  - Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures
  - If appropriate, store any devices involved securely
  - Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk
  - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies)
  - Inform parents/carers about the incident and how it is being managed
  - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using Trust provided or personal equipment
  - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/.
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL (or deputy)
- If learners at other settings are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

Indecent Images of Children (IIOC)

- The academy will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC)
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Kent Safeguarding Child Boards procedures
  - Store any devices involved securely
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy) is informed
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
  - Ensure that any copies that exist of the image, for example in emails, are deleted
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on Trust provided devices, we will:
  - Ensure that the DSL (or deputy) is informed

- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate)
- Ensure that any copies that exist of the image, for example in emails, are deleted
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only
- Report concerns, as appropriate to parents and carers.

- If made aware that a member of staff is in possession of indecent images of children on Trust provided devices, we will:
  - Ensure that the Principal is informed in line with our managing allegations against staff policy
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy
  - Quarantine any devices until police advice has been sought.

Cyberbullying
- Cyberbullying, along with all other forms of bullying, will not be tolerated within the Trust
- The Trust recognises cyberbullying can fall with in peer on peer abuse and will not be tolerated. Further details can be found in the Trust safeguarding policy.

Online Hate
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated and will be responded to in line with existing policies, including those listed in section 1
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures
- The Police will be contacted if a criminal offence is suspected
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or Kent Police.

Online Radicalisation and Extremism
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our Safeguarding and Preventing Extremism & Radicalisation Policies
- If we are concerned that member of staff may be at risk of radicalisation online, the DSL/Principal will be informed immediately, and action will be taken in line with our Safeguarding and Preventing Extremism & Radicalisation Policies.

7. Additional Trust Procedure Regarding Acceptable Use of Information Systems and IT equipment

System Access
- The systems may not be used for private purposes, unless a member of the Executive Team and/or the Principal has given permission for that use and it does not contravene any rule in this policy
- Staff will only be granted access to IT systems once their employment start dates have been confirmed by the Trust Human Resources team and relevant vetting checks have been completed.

Printing
Printing in Trust premises is to be used for business purposes only.

Copyright
- Users must be aware of their legal responsibility to use only licensed software on any system
- Users are not permitted to copy any software application from an academy or Trust computer system for use outside the academy
- The copyright of materials must be respected: Staff will not copy material protected by copyright restrictions and will only use it in accordance with the licence with which it was purchased/supplied.

Storage of Data

- Users are provided with an area on the system in which to save their work; data will be backed up on a regular basis. Storage of personal items on the system is not permitted
- Storing digital copies of films or digital music collections on the system is not permitted unless they have been uploaded by the Network Manager/ICT support staff to the system in accordance with the licences with which they were purchased
- All data must be stored, processed and deleted in line with the Trust's Data Protection policy. The use of unapproved cloud services to store data (e.g. Dropbox, Box etc) is forbidden
- Some documents are governed by user agreements that do not permit their storage on a network; these documents must remain on the original media on which they were sent.

Using Your Own Device

- Users are responsible for their own device/s and use them at their own risk. The Trust is not responsible for any damage, loss or theft of personal devices used on site
- Users wishing to use their own device should ensure it has appropriate and up to date anti-virus software installed
- Personal devices can, however, be configured by the Network Manager/ICT support staff for Wi-Fi access to the internet from Trust sites. The Trust accepts no liability when configuring a personal device for use on its networks; repair or upgrade of a device is the owner's responsibility and will not be undertaken by Trust personnel
- Internet access on personal devices is filtered in the same manner as access on the Trust's devices; users will be required to login using their Trust network credentials or authenticate via Pre-Shared Key in order to access the Internet.

Trust Equipment

- All equipment owned by the Trust is security marked and any mobile devices are assigned to a user who is responsible for that device
- Users are responsible for the equipment that they use. A record of user access to the device is kept and any damage to the equipment will result in a cost incurred by the user for repair or replacement where necessary
- Any equipment that is loaned to a user must be returned either when leaving the Trust's employment or on request by a Line Manager or by the Network Manager. Failure to return equipment will result in a cost incurred by the user
- Staff are responsible for Trust equipment used in classrooms and will check that all devices are working correctly and without damage at the start and end of each lesson
- Any damage, loss or theft of equipment must be reported immediately to the Network Manager/ICT support staff and if there is a risk to data, reported to the Data Protection Officer
- Staff must not attempt to install or download software without the permission of the Network Manager.

Identification (ID) Badges

- ID badges must be worn on site at all times
- In the event that your ID Badge is lost you should immediately notify the issuing party to ensure that the badge is deactivated and replaced
- ID badges must not be lent or passed to another person, whether an employee of the Trust or not
- ID badges must be returned to a member of the Human Resources Team or the IT Network Manager at the end of a member of staff's employment.

POLICY REVIEW AND RATIFICATION

Policy reviewed bi-annually and ratified by the Audit and Risk Committee in December.

This review by the CEO	November 2018
Summary of amendments to this iteration:	1 Amalgamation of the Digital Communications policy and the Information Systems: Acceptable Use policy. 2 Addition of e-safety to the policy.
Ratified by Audit and Risk	December 2018
Next review	July 2020

Appendix One: E-Safety and Information Systems: Acceptable Use Policy Acknowledgement - Staff

E-Safety and Information Systems: Acceptable Use Policy Acknowledgement Staff

Signed in confirmation of policy compliance prior to system access being granted.

Please complete the following in BLOCK CAPITALS, sign and return to the Network Manager or issuing member of staff

Full Name: .....

Staff: .....

Trust / Academy: .....

Position in Trust / Academy: .....

.....

Signature: ..... Date: .....

Access granted by: ..... Date: .....

Brook Learning Trust

Appendix Two: E-Safety and Information Systems: Acceptable Use Policy Acknowledgement - Parents/Carers and Students

<school name> E-Safety and Information Systems: Acceptable Use Policy Acknowledgement

Parent/Carer

I, with my child, have read and discussed <**school name**>'s E-Safety and Information Systems: Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons to safeguard both my child and the schools' systems. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

I, with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that the school will contact me if they have concerns about any possible breaches of the E-Safety and Information Systems: Acceptable Use Policy or have any concerns about my child's safety.

I will inform the school or other relevant organisations if I have concerns over my child's or other members of the school communities' safety online.

I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools online safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

I know that I can approach academy staff (particularly the Designated Safeguarding Lead) and/or a member of the Senior Leadership Team if I have any concerns about online safety (e-safety).

Student

I agree to follow E-Safety and Information Systems: Acceptable Use Policy when:

1. I use school systems and devices, both on and offsite
2. I use my own devices in school, when allowed, including mobile phones, gaming devices, and cameras/I will not use my own devices in school (amend as appropriate)
3. I use my own equipment out of the school, in a way that is related to me being a member of the school community, including communicating with other members of the school, accessing school email, learning platform or website. (amend as appropriate)

Child's Name ……..

Child's Signature ……..

Class…… Date……

Parent's Name ……

Parent's Signature…… Date……

Appendix Three: Visitor/Volunteer Information Systems: Acceptable Use Policy

For visitors/volunteers and staff who require temporary access Trust IT Networks.

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community, including visitors and volunteers, are fully aware of their professional responsibilities and read and sign this Visitor/Volunteer Information Systems: Acceptable Use Policy.

This is not an exhaustive list; visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with Data Protection legislation, including GDPR. Any data which is being removed from the school site, such as via email or on memory sticks or CDs, will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the Trust's Data Protection policy and will always reflect parental consent. (**This statement is only required if visitors/volunteers have access to data**).

2. I have read and understood the Brook Learning Trust E-safety and Information Systems: Acceptable Use Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny.

    - All communication will take place via school approved communication channels such as via a school provided email address or telephone number and not via personal devices or communication channels such as via personal email, social networking or mobile phones.

    - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead (name) and/or Principal.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the Brook Learning Trust E-safety and Information Systems: Acceptable Use Policy and the Law.

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Trust, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, I will raise them with the Designated Safeguarding Lead or the Principal.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke the Staff Disciplinary and Conduct Matters Policy and Procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the <school name> Visitor/Volunteer Information Systems: Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……..

Appendix Four: Wi-Fi Acceptable Use Policy for Visitors/ Volunteers

For those using Trust provided Wi-Fi.

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the schools' boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

1. The school provides Wi-Fi for the school community and allows access for educational use and other business relating to the Trust/academies. The Wi-Fi network is protected by a network password to prevent automatic connections to devices looking for open networks. Once connected users are required to enter a voucher code valid for a set amount of time to access the internet, codes supplied are unique to each individual in order to monitor their internet activity. Internet traffic is filtered in line with our policy for staff; this may mean that some website/services are unavailable.

2. I am aware that the Trust will not be liable for any damages or claims of any kind arising from the use of the wireless service. The Trust takes no responsibility for the security, safety, theft, insurance and ownership of any device used within Trust premises that is not the property of the Trust.

3. The use of ICT devices falls under Brook Learning Trust's E-safety and Information Systems: Acceptable Use Policy, Staff Code of Conduct, Staff Disciplinary and Conduct Matters Policy and Procedure, Allegations of Abuse Against Staff Policy, Behaviour Policy, Safeguarding Policy, Data Protection Policy and Sex, Preventing Extremism and Radicalisation Policy and Relationship Education Policy which all pupils/staff/visitors and volunteers must agree to and comply with.

4. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

5. School owned information systems, including Wi-Fi, must be used lawfully; I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

6. I will take all practical steps necessary to make sure that any equipment connected to the schools' service is adequately secure, such as up-to-date anti-virus software, systems updates.

7. The Trust's wireless is secure to industry standard WPA2-PSK (AES) but we cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. I confirm that I knowingly assume such risk.

8. The Trust accepts no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school's wireless service's connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-

borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

9. The Trust accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the Trust's wireless service.

10. I will respect system security; I will not disclose any password or security information that is given to me. To prevent unauthorised access, I will not leave any information system unattended without first logging out or locking my login as appropriate.

11. I will not attempt to bypass any of the schools' security and filtering systems or download any unauthorised software or applications.

12. My use of Trust Wi-Fi will be safe and responsible and will always be in accordance with the E-safety and Information Systems: Acceptable Use Policy and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

13. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

14. I will report any online safety concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead as soon as possible.

15. If I have any queries or questions regarding safe behaviour online, I will discuss them with Designated Safeguarding Lead or the Principal.

16. I understand that my use of the school Wi-Fi may be monitored and recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with Brook Learning Trust's Wi-Fi Acceptable Use Policy.

Signed: ……..... Print Name: …… Date: …….

Appendix Five: Key Academy Contacts, Kent Support and Guidance for Educational Settings

Academy Designated Safeguarding Lead:
<Insert DSL name and contact details>

Education Safeguarding Team:
Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Ashley Assiter, Online Safety Development Officer
Tel: 03000 415797

Guidance for Educational Settings:

- https://www.kelsi.org.uk/child-protection-and-safeguarding
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials
- www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-useful-links
- Kent Online Safety Blog: www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

KSCB: www.kscb.org.uk

Kent Police: www.kent.police.uk or https://www.kent.police.uk/advice/online-safety/
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Kent Police via 101.

Other:
Kent Public Service Network (KPSN): www.kpsn.net
EiS - ICT Support for Schools and Kent Schools Broadband Service Desk: www.eiskent.co.uk

National Links and Resources for Educational Settings:
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk
Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers:
Action Fraud: www.actionfraud.police.uk
CEOP: www.thinkuknow.co.uk www.ceop.police.uk
Childnet: www.childnet.com
Get Safe Online: www.getsafeonline.org
Internet Matters: www.internetmatters.org
Internet Watch Foundation (IWF): www.iwf.org.uk
Lucy Faithfull Foundation: www.lucyfaithfull.org
NSPCC: www.nspcc.org.uk/onlinesafety
ChildLine: www.childline.org.uk
Net Aware: www.net-aware.org.uk
The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
UK Safer Internet Centre: www.saferinternet.org.uk