South Farnham Educational Trust

The Continual Pursuit of Excellence

ONLINE SAFETY & ACCEPTABLE USE POLICY

REVIEW: ANNUALLY

LAST REVIEW DATE: SUMMER 2024

Introduction

The Online Safety & Acceptable Use Policy has been written based on best practice and government guidance in consultation with the Senior Leadership Team and Local Governing Body and has been approved by Trustees. The policy and its implementation will be reviewed annually. The policy covers the use of all technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and handheld games consoles used on the school site.

The Online Safety & Acceptable Use Policy recognises that there are differences between the use of technology as a private individual and as a member of staff or as a pupil.

Online Safety is part of the school's safeguarding responsibilities. This policy relates to other policies including the Social Media Policy, Behaviour Policy, Safeguarding Policy and Data Handling Policy.

Aims

Great Bookham School aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and Guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and Health Education
- Searching, screening and confiscation

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

The policy reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.

In addition, the policy reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

South Farnham Educational Trust
The Continual Pursuit of Excellence

The four key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention. to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Roles and Responsibilities

Managing access and security

Great Bookham School will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between our systems and networks and the more open systems outside school. Annual staff training will include a session on recognising phishing attempts and how to set a strong password/password security.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age-appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal passwords.**
- Accounts are protected from cyber-attacks by enabling and enforcing MFA and where not possible using reduced sign in attempts and/or restricting access by IP address. A decision is made for each service depending upon the security capabilities.
- Where biometric authentication is not possible, users must have a strong password to unlock their device. This should consist of a minimum of 12 characters (with no maximum length restriction), including upper and lower-case letters, special characters and numbers.
- Off-site access to the school network will be controlled by multi-factor authentication (MFA).
- Systems will be in place to ensure that internet use can be monitored, and a log of any incidents will be kept to help to identify patterns of behaviour and to inform future Online Safety policies (CPOMs or appendix 5).
- If a user believes their password to have been compromised, they must immediately inform their line manager and the IT Support Desk. The user will be forced to change their password using the web GUI and the IT support desk will log the incident through a ticket system.
- Work devices used off-site must not be used by family or friends and solely for work activities.

- If staff have any concerns over the security of their device, they must seek advice from the IT manager/lead.
- The security of our systems and networks will be reviewed regularly.
- All staff that manage filtering and monitoring systems will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Local Governors' responsibilities for filtering and monitoring:

- Hold the Headteacher to account for implementation of this policy.
- Make sure the DSL responsibilities are understood and monitored.
- Ensure staff training has been completed and that staff have a clear understanding of their roles and responsibilities.
- Review the DfE's filtering and monitoring standards.
- Review filtering and monitoring provision on an annual basis (ensuring termly checks are completed by the school).
- Assign a Local Governor to be responsible for filtering and monitoring.

Headteacher's responsibilities for filtering and monitoring:

- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- Ensure the DSL takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role.
- Ensure that all staff undergo online safety training as part of child protection and safeguarding training.
- Make sure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of their safeguarding training.
- Review the DfE's filtering and monitoring standards.
- Identify and assign roles and responsibilities.
- Ensure that any online safety incidents are logged (CPOMs or appendix 5) and dealt with appropriately in line with this policy/Safeguarding and Child Protection policy.
- Ensure that the school has put an appropriate level of security protection in place and that procedures, such as filtering and monitoring systems on school devices and school networks, are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Review filtering and monitoring provision on a termly basis.
- Block harmful and inappropriate content without unreasonably impacting T&L.

- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Have effective monitoring strategies in place that meet their needs.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Discuss with IT staff and service provider what needs to be done to support the school.
- Assign a member of SLT and a Local Governor to be responsible for filtering and monitoring.

The Designated Safeguarding Lead (DSL) responsibilities:

Details of the school's designated safeguarding lead (DSL) and DSL team are set out in the Child Protection and Safeguarding Policy, as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher and Local Governing Body to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager/lead to make sure the appropriate systems and processes are in place
- Working with the Headteacher, ICT manager/lead and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Child Protection and Safeguarding Policy.
- Ensuring that any online safety incidents are logged (CPOMs or appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety (appendix 4 contains an example self-audit for staff on online safety training needs).
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or Local Governing Body.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

All staff's responsibilities for filtering and monitoring:

- Maintain an understanding of this policy.
- Implement this policy consistently.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendices 1 & 2) and ensuring that pupils follow the school's terms on acceptable use (appendix 3).

- Monitor what is on pupils' screens.
- Teach pupils about online safety.
- Know that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by reporting directly to the DSL and/or Headteacher.
- Follow the correct procedures if they need to temporarily bypass the filtering and monitoring systems for educational purposes.
- Work with the DSL to ensure that any online safety incidents are logged (CPOMs or appendix 5) and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Respond appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'. Know how to report safeguarding and technical concerns, if:
    - You witness or suspect unsuitable material has been accessed.
    - You are able to access unsuitable material.
    - You are teaching topics that could create unusual activity on the filtering logs.
    - There is failure in the software or abuse of the system.
    - There are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
    - You notice abbreviations or misspellings that allow access to restricted material.

Parents'/Carers' responsibilities for filtering and monitoring:

- Engage with support and guidance provided by the school to ensure that home devices have appropriate levels of filtering and monitoring in place.
- Monitor their children's online activity, including mobile phone use, to ensure that they are behaving responsibly and appropriately online.
- Notify the school with any concerns or incidents relating to inappropriate activity online or any concerns/queries relating to this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 3).

The school will endeavour to raise parents/carers' awareness of online safety in letters or other communications home, as well as providing up-to-date information via the school website. This policy will also be shared with parents/carers. Online safety will also be covered during parents' information and collaboration evenings.

The school will inform parents/carers of:

- The systems that the school uses to filter and monitor online use.
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

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

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

Educating Pupils About Online Safety - Curriculum

Great Bookham School will provide an age-appropriate Online Safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety (including age restrictions, content and personal data). Government guidance is considered with reference to the education for a connected world framework (for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives).

Pupils will be taught about Online Safety as part of the curriculum. All schools must teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

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

Pupils in **Key Stage (KS) 2** will be taught to:

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

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

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.

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

Pupils in **Key Stage (KS) 3** will be taught to:

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

Pupils in **Key Stage (KS) 4** will be taught to:

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

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

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

The safe use of social media and the internet will also be covered in other subjects where relevant, including through the tutor programme and Head of Year assemblies where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Authorisation of Access

- All staff (including teaching staff, teaching assistants, support staff, office staff, trainee teachers, work experience trainees, ICT technicians and governors) must read and sign the Acceptable Use of Computers, IT Equipment, Internet and Email (Staff) Policy before accessing our systems and networks (Appendices 1 and 2).
- Account creation is triggered by HR processes during the recruitment/induction process. New accounts must be approved by a responsible person who sits at Executive Trust level prior to creation on any systems.
- On joining, staff are granted least privilege rights based on role-based permissions. Access control is reviewed annually and when staff change roles within the organisation. Staff that require additional access must be approved by the Deputy CEO. All changes are documented.
- All privileges are immediately revoked when a member of staff leaves the organisation. HR will complete a 'leavers' process to trigger the disabling of an account on, or before, the last day of employment.
- All administration level accounts are kept strictly for administration purposes, not day-to-day working, and by permission of the central trust team. Staff using these administration accounts receive training and only use the credentials to make planned system changes. Mailboxes are not linked to administration accounts and MFA is used to secure these accounts.
- The school will maintain a current record of all staff and pupils who are granted access to our systems and networks.
    - **At Key Stage 1**, access to the internet will be by adult demonstration with supervised access to specific, approved online material, which supports the learning outcomes planned for the pupils age and ability.
    - **At Key Stages 2**, **3** and **4** access to the internet will be with teacher permission and supervision but with increasing levels of autonomy, using age-appropriate search engines and online tools.
- People not employed by the school must read and sign the Acceptable Use of Computers, IT Equipment, Internet and Email (Visitors) Agreement (appendix 2) before being given access to the internet via school equipment.
- Parents/carers will be asked to sign and return a consent form (Acceptable Use of the School Computers) to allow use of technology by their child (appendix 3).

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Surrey/Hampshire County Council can accept liability of the material accessed or any consequences of internet access.

Protocols

Email

- Staff may only use approved email accounts on our systems and networks.
- Incoming email should be treated as suspicious, and attachments should not be opened unless the author is known.
- Pupils will be given restricted email accounts in line with safeguarding procedures.

Published Content – e.g. School Website, school social media accounts

- The contact details will be the school address, email and telephone number. Staff and pupil's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school website or any school run social media as set out in the Surrey/Hampshire Safeguarding Children Board Guidance on using images of children.

Use of social media including the school learning platform

- The school has a separate social media policy.
- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Use of video services such as Zoom or Teams will be monitored by staff and will be limited to class-based activities.
- Staff and pupils should ensure that their online activity both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the community.

Use of personal devices

- Personal equipment may be used by staff to access our systems and networks provided their use complies with this Policy.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to school systems.

Handling Online Safety Complaints

- Complaints of internet misuse will be dealt with according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school behaviour policy.

Harms and Risks

Navigating the Internet and Managing Information

- Pupils will learn how to navigate the internet safely as part of their Computing/Computing Science lessons.
- Due to the complex nature of the internet, pupils will be encouraged to consider information presented to them with caution, ensuring that they consider the reliability of the source.
- Topics will include considering age restrictions, disinformation/misinformation, fake websites and scam emails, online fraud and personal data (including protecting passwords and privacy settings).

Staying Safe Online

- Alongside the Computing/Computer Science curriculum content, pupils will learn how to stay safe online from outside agencies, including the Police and the NSPCC.
- Pupils will receive age specific advice covering the following topics:
    - online abuse (e.g. sexual harassment, bullying, trolling and intimidation)
    - online challenges and identifying whether they are safe or not
    - content which incites
    - fake profiles (i.e. adults posing as children or 'bots')
    - grooming (e.g. radicalisation, Child Sexual Abuse and Exploitation and gangs)
    - risks linked to live streaming
    - interacting with known contacts to avoid unsafe communication

Wellbeing

- At Great Bookham School, we ensure that pupil's wellbeing is continually monitored through discreet PSHE lessons, including Relationships Education, and opportunities where pupils can voice their concerns.

- As part of this learning, pupils will look specifically at online safety relating to screen time use and allowances, and how people's behaviour can differ online and offline.

- These lessons will be conducted in a safe and trusting manner, where pupils will be encouraged to follow the 'SMART' guidance for staying safe online.

Cyber-bullying

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

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

- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
- The school will send information on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.
- The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The school recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The school will treat any use of AI to bully pupils in line with our antibullying and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Communication of the Policy

To Pupils

- Pupils need to agree to comply with this policy to gain access to our systems and networks and to the internet (Acceptable Use document: appendix 3).
- Pupils will be reminded of the contents of this policy as part of their Online Safety education.

To Staff

- All staff will be provided with access to the Online Safety & Acceptable Use Policy and its importance will be explained.
- All staff must sign and agree to comply with this policy to gain access to the school's systems and networks and to the internet (Acceptable Use document: appendix 1).

To Visitors and Volunteers

- All visitors or volunteers must sign and agree to comply with this policy to gain access to the school's systems and networks and to the internet (Acceptable Use document: appendix 2).

To Parents

- The school will ask all new parents to sign the parent/pupil agreement when they register their child with the school (appendix 3).
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters and on the school website.
- Parents will be offered Online Safety training annually.

Mobile Technology Guidance

Staff and Visitors use of personal devices

- Mobile phones and personally-owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Mobile phones and personally-owned devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile phones or devices.
- No images or videos should be taken on mobile phones or personally-owned devices, including on school trips or out of school activity – only school provided equipment will be used for this purpose.
- Staff are not permitted to use their mobile phones or personal devices for contacting pupils, young people or those connected with the family of a student.

- If a member of staff breaches the school's policy, then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to the lunchbreak and after school.

Pupil use of mobile devices

Please refer to the school behaviour policy for specific details about the use of mobile phones in school.

- Parents wishing for their child to bring a mobile phone into school must notify the school and give their permission in advance. Pupils must then hand their device into the office on arrival. No mobile phones or personal devices including Smart watches are to be kept in classrooms or cloakrooms during school hours – the only exception being those requiring their mobile phone to monitor medical support systems such as Dexcom diabetes monitoring systems.
- Pupils should protect their mobile phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices.
- If a pupil breaches the school's policy, then the phone or device will be confiscated and it will be held in a secure place in the school office. Mobile phones and devices will be released to parents and carers in accordance with school policy.

Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or is evidence in relation to an offence.
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
    - Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the DSL and/or Headteacher.
    - Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
    - Seek the pupil's co-operation.

- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
    - Cause harm, and/or undermine the safe environment of the school or disrupt teaching, and/or
    - Commit an offence.

- If inappropriate material is found on the device, it is up to DSL or other members of the Senior Leadership Team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
    - They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
    - The pupil and/or the parent/carer refuses to delete the material themselves.
- If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:
    - Not view the image
    - Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Any searching of pupils will be carried out in line with:
    - The DfE's latest guidance on searching, screening and confiscation.
    - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
    - Our behaviour policy / searches and confiscation policy.
    - Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Vulnerable Children

- Any pupil can be vulnerable online, and their vulnerability is affected by their age, developmental stage and personal circumstance.
- Great Bookham School 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.
- Great Bookham School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum, Great Bookham School will seek input from specialist staff as appropriate, including the SENCO.

South Farnham Educational Trust
The Continual Pursuit of Excellence

Useful Links for Educational Settings

National Organisations for Schools

- The Anti-Bullying Alliance: www.anti-bullyingalliance.org.uk
- Childnet: www.childnet.com
- DotCom Digital: https://dotcomdigital.co.uk/
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation: www.iwf.org.uk
- NSPCC: www.nspcc.org.uk/onlinesafety
- UK Safer Internet Centre: www.saferinternet.org.uk
    - 360 Degree Safe: www.360safe.org.uk

National Organisations for Parents/Carers

- Internet Matters: www.internetmatters.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- Parent Info (CEOP and Parent Zone): https://parentinfo.org
- Parent Zone: https://parentzone.org.uk/parents

National Organisations for Pupils

- BBC Own It: https://www.bbc.com/ownit includes links to their Own It app.
- Childline: www.childline.org.uk

Appendices

Appendix 1: Acceptable and Responsible Use of Computers, IT Equipment, Internet and Email Agreement (Staff)

Appendix 2: Acceptable and Responsible Use of Computers, IT Equipment, Internet and Email Agreement (Visitors, Governors and Volunteers)

Appendix 3: Acceptable and Responsible Use of Computers, IT Equipment, Internet and Email Agreement (Pupil and Parent/Carer)

Appendix 4: Online safety training needs audit (optional template)

Appendix 5: Online safety incident report log (for schools without access to CPOMs)

South Farnham Educational Trust

The Continual Pursuit of Excellence

Appendix 1

Acceptable and Responsible Use of Computers, ICT Equipment, Internet and Email Agreement (Staff)

The Computer Network (including laptops and other ICT peripherals) is owned by the school. This statement helps to protect staff by clearly stating what use of computer resources is acceptable and what is not. The use of any part of the Computer Network without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

1. All network access must be made via the user's authorised account and password, which must not be given to any other person.
2. All users accounts can and will be monitored as directed by the Head Teacher or CEO/Deputy.
3. School computer use and Internet use must be appropriate to staff professional activity. Where laptops have been provided, they may be used outside the school's premises for professional activities only. Laptops are not covered by the school's insurance when they are off school property. They must not be left unattended at anytime, both on and off school premises.
4. All users must follow guidance and set a strong password to unlock their device. This should consist of a minimum of 12 characters (with no maximum length restriction), including upper and lower-case letters, special characters and numbers.
5. All users must immediately report potentially compromised passwords to their line manager and IT support desk. The user will be forced to change their password using the web GUI and the IT support desk will log the incident.
6. School systems and resources must not be used under any circumstances for the following purposes:

    - to communicate any information that is confidential to the school or to communicate/share confidential information which the member of staff does not have authority to share.
    - to present any personal views and opinions as the views of the school, or to make any comments that are libellous, slanderous, false or misrepresent others.
    - to access, view, download, post, email or otherwise transmit pornography, sexually suggestive or any other type of offensive, obscene or discriminatory material.
    - to communicate anything via ICT resources and systems or post that may be regarded as defamatory, derogatory, discriminatory, harassing, bullying or offensive, either internally or externally.
    - to communicate anything via ICT resources and systems or post that may be regarded as critical of the school, the leadership of the school, the school's staff or its pupils.
    - to upload, download, post, email or otherwise transmit or store material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
    - to collect, store or send personal information about children or adults without direct reference to The Data Protection Act/GDPR.
    - to use the school's facilities to undertake any trading, gambling, other action for personal financial gain, or political purposes, unless as part of an authorised curriculum project.
    - to use the school's facilities to visit or use any online messaging service, social networking site, chat site, web-based email or discussion forum not supplied or authorised by the school.
    - to undertake any activity (whether communicating, accessing, viewing, sharing. uploading or downloading) which has negative implications for the safeguarding of children and young people.

Any of the above activities are likely to be regarded as gross misconduct, which may, after proper investigation, lead to dismissal. If employees are unsure about the use of ICT resources including email and the intranet, advice should be sought from a member of the Senior Leadership Team or Computing Co-ordinator/Lead if applicable.

7. Copyright and intellectual property rights must be respected.

8. The use of personal email accounts within school is strictly prohibited. Certain members of staff are provided with a school email account which can be used for communication with third party as directed by the Head Teacher.

9. All email accounts are monitored by the Head Teacher, supported by the ICT Technician/Lead. Emails should be written carefully and politely and authorised before sending, in the same way as a letter written on school headed paper.

10. The forwarding of chain letters via email is not permitted.

11. All administration level accounts are strictly for administration purposes only, not day-to-day working, and by permission of the central trust team. Mailboxes must not be linked to administration accounts and MFA must be used to secure these accounts.

12. In accordance with the procurement procedures of the school, individuals must not order items via the Internet or by email. Any orders must be processed by the designated office staff.

13. The use of Internet Chat rooms, Instant messaging services and Internet Notice Boards is strictly prohibited unless authorised for professional activity by the Head Teacher. Microsoft Teams is an exception.

14. The use of portable media such as floppy disks, memory sticks and CD-ROMs is not allowed without permission from the Head Teacher or Computing Coordinator/Lead.

15. Downloading or installing applications or software from the Internet or from CD-ROMs is not permitted.

16. Computers, particularly laptops, will be regularly serviced by the ICT Technician. Please tell the Computing Coordinator/Lead or ICT Technician immediately if you have concerns about a machine.

17. I understand that by using a personal electronic device, I will need to ensure that the device is kept up to date and is not jailbroken or modified in any way.

18. I understand that I am responsible in ensuring that my device is password protected and I only access school data via the web browser and not sign into any third-party applications or office applications. This includes but is not limited to Office 365, Mail, Contacts, Calendars.

19. Staff should consider carefully if they need a hardcopy of a document before they print, especially if they are printing a large, coloured document.

20. Pupils will only use school ICT systems or the internet when a teacher is present (primary and KS3), or with a teacher's permission (KS4).

21. Peripherals are kept in the ICT Technician's office which is out of bounds to all staff except: the Head Teacher, the ICT Technician, the Computing Coordinator and other individuals granted permission by the Head Teacher.

22. Digital cameras and digital videos may only be used for school activities. Care must be taken when taking photographs of children which may only be used within the school. If photographs are required for external presentations, the Head Teacher must be consulted before they are used. After using the digital cameras/videos, any photographs should be stored appropriately on the system and the SD card cleared before returning the camera to its storage location.

23. Personal cameras, including Smartphones are not permitted for the usage of photographing children.

24. Smartphones are not permitted to be used for the sending or receiving of school related data and information, unless the device has been provided by the Academy Trust.

25. Take care around all ICT equipment, always follow safety advice and report any breakages or problems, however minor they may seem, immediately to the Computing Coordinator/Lead or ICT Technician.

Declaration of Understanding:

I confirm that I have read and understood the **Acceptable and Responsible Use of Computers, ICT Equipment, Internet and Email Agreement (Staff).** I understand that the school may exercise its right to monitor the use of the

school's computer systems, including access to web sites, the interception of email and the saving and retrieval of files contained in the Network User areas and on laptops. I accept receipt of the laptop below on the understanding it is for professional use only and the school has the right to request the return with immediate effect wherever it sees fit.

Signed .....

Name in Print .....

Laptop Number .....

Date .....

South Farnham Educational Trust
The Continual Pursuit of Excellence

Appendix 2

Acceptable and Responsible Use of Computers, ICT Equipment, Internet and Email Agreement (Visitors, Governors and Volunteers)

The Computer Network (including laptops and other ICT peripherals) is owned by the school. This statement helps to protect visitors, governors and volunteers by clearly stating what use of computer resources is acceptable and what is not. The use of any part of the Computer Network without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable):

1. I understand that I have been given use of the school internet and/or the school's systems and networks in order to carry out a specific job for the school.
2. I understand that it is a criminal offence to use the systems and networks for a purpose not permitted by its owner.
3. I will use the school's systems and networks for the purpose for which I have been given access.
4. I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
5. I will not install software or connect unauthorised hardware or devices to the school's network without the permission of the Headteacher and Computing Coordinator/Lead.
6. I will not access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material).
7. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school's systems and networks.
8. I will not access or use social networking sites.
9. I will not take photographs that include pupils within the school without permission from the Headteacher.
10. I understand that all my use of the internet and other related technologies can be monitored and logged and it can be made available, on request, to the Headteacher or my employer.
11. I will respect copyright and intellectual property rights.
12. I will not access, modify or share data I am not authorised to do.
13. I will not promote private businesses, unless that business is directly related to the school.
14. I understand that if I disregard any of the above then it will be reported to the Headteacher or my employer and serious infringements may be referred to the police.

Declaration of Understanding:

I confirm that I have read and understood the **Acceptable Use of Computers, IT Equipment, Internet and Email Agreement and Online Safety Policy**. I understand that the school may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of email and the saving and retrieval of files contained in the Network User areas and on laptops.

Full name in print .....

Company .....

Signed .....

Date .....

South Farnham Educational Trust
The Continual Pursuit of Excellence

Appendix 3

Acceptable and Responsible Use of Computers, ICT Equipment, Internet and Email Agreement (Pupil and Parent/Carer)

Dear Parent/Carer,

All pupils at Great Bookham School will use the ICT systems and computer facilities, including the Internet, as part of their learning and as required by the National Curriculum. The school takes every reasonable precaution to keep pupils safe and to prevent them from accessing inappropriate materials.

These steps include:

- a filtering system
- a monitoring system
- vigilant oversight of pupils' computer files and internet access
- the teaching of Online Safety
- the requirement that pupils and parents/carers observe online safety rules

Computing provides an exciting and challenging learning opportunity for the children that embraces the technology and methodology which is such an important part of our world.

We would like both pupils and parents/carers to sign the agreements to show that the Online Safety rules have been read and understood.

Please would you be so kind as to read, sign and return the agreements attached to the school office.

Yours Sincerely,

Miss J Allen
Headteacher

South Farnham Educational Trust

The Continual Pursuit of Excellence

Acceptable and Responsible Use of Computers, ICT Equipment, Internet and Email Agreement (Pupil and Parent/Carer)

As a pupil of Great Bookham School:

When I use the school's ICT systems, devices and internet:

1. I will take care of the school computers and devices.
2. I will tell an adult straight away if something is broken or not working properly.
3. I will only use the username and password I have been given.
4. I will not give my username and/or password or any personal information to anyone, including my friends.
5. I will only use the Internet when I have been given permission by an adult.
6. I will only use websites provided by a teacher or a teaching assistant.
7. I will tell an adult if I see anything that makes me uncomfortable, worried or unsure.
8. I will tell an adult immediately if:
   - I select a website by mistake.
   - I receive messages from people I don't know.
   - I find anything that may upset or harm me or my friends.
9. I will always be kind, polite and friendly when I write messages on the internet.
10. I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

As a parent/carer of a pupil at Great Bookham School:

1. I have discussed the Pupil Agreement with my child to ensure their understanding.
2. I accept that, ultimately, the school cannot be held responsible for the nature and the content of materials accessed through the internet, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.
3. I understand that the school is not liable for any damages arising from my child's use of the internet facilities.
4. I will support the school by promoting safe use of the Internet and digital technology at home and I will inform the school if I have any concerns over my child's Online Safety.
5. I will not distribute any photographic images of children on social media networks or using any other photographic format.

Pupil's Name: .....

Parent /Carer Name: .....

Parent /Carer Signature: .....

Date: .....

Please complete, sign and return to the school office

South Farnham Educational Trust
The Continual Pursuit of Excellence

Appendix 4

Online safety training needs – self-audit for staff (optional)

Name of staff member/volunteer:	
Date:	

Question:	**Yes/No** (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

South Farnham Educational Trust
The Continual Pursuit of Excellence

Appendix 5

Online safety incident report log

CPOMs should be used to log all online safety incidents. This form should be used by schools without access to CPOMs.

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident