Sandown Primary School and Nursery

Online Safety Policy

Policy Contact Person	Mr. Charlie Lindsay
Review Frequency	Annually
Signed by Approver	
Date Agreed/Signed	September 2023
Next Review Date	September 2024
Signed original stored in Business Manager's Office	

East Sussex County Council

Online Safety Policy

THE BEST THAT WE CAN BE
SANDOWN PRIMARY SCHOOL & NURSERY

Key Details:

Designated Safeguarding Lead(s): Kate Tugwell - DSL / Deputy Head

Named Governor with lead responsibility: Mrs Hayley Cross

Date agreed and ratified by Governing Body: September 2023

Date of next review: September 2024

Contents

Important information

There is no change table to accompany this new policy however there is highlighting, to indicate where things have changed.

When personalising this online safety policy statement schools should consider the following guidance documents:

- Keeping Children Safe in Education, 2023
- Behaviour in Schools: advise for headteachers and school staff 2022
- Teaching Online Safety in Schools: January 2023
- Meeting digital and technology standards in schools and colleges 2023
- Education for a Connected World Framework
- Project Evolve
- Sharing nudes and semi-nudes: advise for education settings working with children and young people
- Harmful online challenges and online hoaxes
- Questions from the governing board
- Keeping Children safe in out of school settings
- Resources on czone, to support primary schools with delivery of the Connected World
- The Statutory framework for the early years foundation stage framework (Jan 2024)
- Safeguarding children and protecting professionals in early years settings: online safety considerations

1. Policy Aims

- This online safety policy has been adapted by Sandown School and Nursery involving staff, learners, governors and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education 2023, Early Years and Foundation Stage and the East Sussex Safeguarding Children Partnership procedures.
- The purpose of this online safety policy is to:
    - Safeguard and protect all members of our community online.
    - 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.
- We identify that the issues classified within online safety are considerable, but can be broadly categorised into four 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.

- **Commerce/Contract:** risks such as online gambling, inappropriate advertising, phishing and or financial scams and sextortion (online sexual coercion and extortion of children).

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledge its duty to ensure that all learners and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- We believe 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 the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (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 school issued devices for use off-site, such as a work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to a member of the school/academy. The Behaviour in Schools guidance (2022) further reinforces this stating: *Maintained schools and academies' behaviour policies should set out what the school will do in response to noncriminal poor behaviour and bullying which occurs off the school premises or online and which is witnessed by a staff member or reported to the school,*
- In this respect the school will deal with such incidents within this policy and associated behaviour and anti-bullying policies to such extent as is reasonable and will, where known, inform parents/carers of incidents of inappropriate

online safety behaviour that has taken place out of school. Action can only be taken over issues covered by the published Behaviour Policy

2.1 Links with other policies and practices

- This policy **links** with several other policies, practices and action plans including:
- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Child protection policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security

2.2 Online safety in community activities, after-school clubs and tuition

- When our school hires out or lets school facilities/premises to organisations or individuals (e.g. community groups, sports associations and service provider to run community or extra-curricular activities), we ensure that appropriate arrangements are in place to keep children safe.
- We seek assurances that where services or activities are provided separately by another body (not under direct supervision or management of our school staff) there are appropriate safeguarding and child protection policies and procedures in place (including online safety) and will inspect these as necessary. This applies regardless of whether or not the children who are attending these services are on our school roll.
- Safeguarding arrangements are clearly detailed in any transfer of control agreement (i.e. lease or hire agreement).

- The DfE has published *Keeping Children Safe during community activities, after-school clubs and tuition* for organisations and individuals who provide these activities for children and young people and this document contains a section on online safety which makes clear that the provider should have an online safety policy or acceptable use policies in place as well as appropriate filtering and monitoring. A staff behaviour policy should also include information on relationships and communications between children (and parents) and staff/volunteers, including the use of social media.

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; We will review this policy at least annually
  - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL Kate Tugwell DSL has lead responsibility for online safety.
  - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.

- The digital and technology standards in schools guidance states that the governing body should identify and assign a member of the leadership team and a governor to be responsible for ensuring these standards are met. The governor responsible for this is Mrs Hayley Cross.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team and governors will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure that online safety is a running and interrelated theme whilst devising and implementing the whole school approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies (including the staff code of conduct and/or acceptable use policies) and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.
- Ensure that they are doing all that they reasonably can to limit children's exposures to risks from the school's IT system and therefore have appropriate filtering and monitoring systems in place. They will have an awareness and understanding of the provisions in place and will work with technical staff to monitor the safety and security of our systems and networks.

- Ensure that all relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively as well as knowing how to escalate concerns when identified.
- Ensure that they regularly review the effectiveness of filters and monitoring systems; as schools increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material (including when they are online at home).
- Ensure that the DfE's filtering and monitoring standards for schools and colleges are being met: this will be supported through using the checklist appended to this policy.
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.
- Support the DSL and any deputies by ensuring they have the additional time, funding, training, resources and support they need to carry out the role effectively.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Audit and evaluate online safety practice, annually, to identify strengths and areas for improvement.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology that considers and reflects the risks our children face.

- Communicate with parents regarding the importance of children being safe online, the systems being used in school and information regarding what their children are being asked to do online by the school.

4.2 The Designated Safeguarding Lead (DSL) will:

- Be an appropriate senior member of staff from the school leadership team.
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Liaise with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep learners safe online
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.

- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.

  Report online safety concerns, *to the SLT and Governing Body*.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input, including from pupils.
- Meet regularly (termly) with the governor with a lead responsibility for safeguarding *and* online safety.

4.3 It is the responsibility of all members of staff to:

- Be aware that technology is a significant component of many safeguarding and wellbeing issues and that children are at risk of abuse online as well as face to face and that in many cases abuse will take place concurrently via online channels and in daily life.
- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Proactively monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and consistently implement current policies with regard to these devices

- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Ensure that students are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Reinforce the school's online safety messages when teaching lessons online

4.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures and compliance with DfE's filtering and monitoring standards for schools and colleges.
- Implement appropriate security measures *such as password policies and encryption)* to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

4.5. It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities provided by the school/setting.
- Contribute to the development of online safety policies.
- Read and adhere to Acceptable Use Policies, which are appended to the end of this policy.

- Understand the importance of good online safety practice out of school and understand that this policy covers their actions outside of school if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult or other support services, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the Acceptable Use Policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the Acceptable Use Policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- We will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home 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) and computing programmes of study (Purple Mash / Jigsaw)
    - 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. This should include the use of generative AI tools and services.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- We will support learners to read and understand the Acceptable Use Policies in a way which suits their age and ability by:
    - Displaying age-appropriate acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation. This should include information about whether school-owned devices are also monitored when not connected to the school network.
    - Rewarding positive use of technology using dojo.

- Implementing appropriate peer education approaches. This includes Digital Leaders. ○ Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- We recognise 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.
- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. We will use accessibility tools to aid the use of tech devices by pupils with SEND.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher. This will include Mrs Gail Harley.

5.3 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 and governors on a regular basis, with at least annual updates.
    - This will be as part of existing safeguarding and child protection training/updates or within separate or specific online safety sessions.
    - This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- 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 setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- 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.

5.4 Awareness and engagement with parents and carers

- We recognise 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 parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.
- Providing them with information about our approach to filtering and monitoring as well as information about the types of things that children will be doing online.

6. 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 (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.
- All members of the community will be directed to the DSL or Headteacher in such circumstances.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- 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.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, should be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
- Where there is suspicion that illegal activity has occurred contact the Sussex 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 headteacher will contact Sussex Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Learners' Welfare

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

6.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher in accordance with the allegations policy.

- For any allegations regarding a member of staff's online conduct a consultation will be sought with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

7. Procedures for Responding to Specific Online Incidents or Concerns

7.1 Child-on-child online sexual violence and sexual harassment

Our setting has accessed and understood part 5 of Keeping Children Safe in Education September 2023.

- We recognise that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here'. Examples may include; non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, upskirting, 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 child protection and anti-bullying policy.
- We recognise 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.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

- We 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. This will be via our Jigsaw PSHE programme.
- 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 Care 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 Sussex 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.

7.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')

- We recognise youth produced sexual imagery (known as "sharing nudes and semi nudes") 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 UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or 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/off site or using setting provided or personal equipment.

- We will not:
  - View any images suspected of being youth produced sexual imagery, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented– **in most cases, images or videos should not be viewed.** The UKCIS/DSIT guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people provides information on the steps to be taken if an image does need to be viewed.
  - 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 policy.
  - Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and 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 Care and/or the Police, as appropriate.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support. This will include signposting to services such as *report remove* and *take it down*

  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 UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and 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.

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

- We 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.
- We recognise 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. This can be found on the school website on the computing tab.

- 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 East Sussex Safeguarding Child Partnership's procedures.
    - If appropriate, store any devices involved securely.
    - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
    - Carry out a risk assessment which considers any vulnerabilities of pupil(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 setting 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 Police.
- If learners at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

7.4 Indecent Images of Children (IIOC)

- We 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 implements 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 the Police.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy. ○ Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex 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 DSL) is informed, who will investigate the incident.
    - 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 the setting provided devices, we will:
    - Ensure that the DSL (or deputy DSL) and Headteacher are 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 once directed to by the police.

  - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
  - 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 setting provided devices, we will:
  - Ensure that the Headteacher 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.

7.5 Cyberbullying

- All staff will understand that children are capable of abusing their peers online. Cyberbullying, along with all other forms of bullying, will not be tolerated here.
- Full details of how we will respond to cyberbullying are set out in our antibullying policy. Found on the school website.

7.6 Cybercrime

- We will ensure that all members of the community are aware that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.
- If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), will consider referring into the Cyber Choices programme.
- We will seek advice from Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

7.7 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at our setting and will be responded to in line with existing policies, including anti-bullying and behaviour.
- 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 DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

7.8 Online Radicalisation and Extremism

- We will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation
- 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. Our Smoothwall Filtering and Monitoring site will ensure all inappropriate sites cannot be accessed and are blocked.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff or governor may be at risk of radicalisation online the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

8. Safer Use of Technology

8.1 Classroom Use

- We use a wide range of technology. This includes access to:

- Computers, laptops, tablets and other digital devices
- Internet which may include search engines and educational websites ○ Learning platform/intranet ○ Email
- Games consoles and other games-based technologies ○ Digital cameras, web cams and video cameras

- All devices will be used in accordance with our Acceptable Use Policies 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.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- 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.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools. *(Amend as appropriate)*
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.
  - **Key Stage 3, 4, 5**
    - Learners will be appropriately supervised when using technology, according to their ability and understanding.
  - **Learners in residential provision**

- 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 in accordance with the national minimum standards (NMS).

8.2 Managing Internet Access

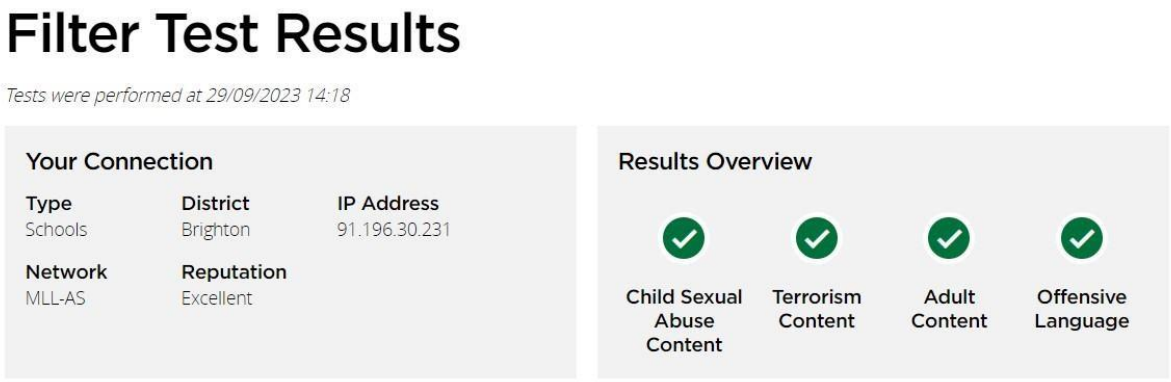
- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

8.3 Filtering and Monitoring

 The school is compliant with the DfE's filtering and monitoring standards for schools and colleges. This is checked and reviewed at least annually using the checklist appended to this policy.

8.3.1 Decision Making

- Our governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.



- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances and is reviewed at least annually by the DSL, IT service provider and the governor responsible for safeguarding/online safety. A review will also be carried out following the identification of a safeguarding risk or any changes in working practice such as remote access or Bring Your Own Device or if new technology is introduced. We follow the guidance outlined in the DfE filtering and monitoring standards when carrying out the review.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, 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 using the Safer Internet Centre guidance on appropriate filtering and appropriate monitoring.
- 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.

8.3.2 Decision Making

- Education broadband connectivity is provided through East Sussex County Council.
- We use Smoothwall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- We work with East Sussex County Council and Smoothwall to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
    - Insert details of the procedure here e.g. turn off monitor/screen and 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 deputies) 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, Sussex Police or CEOP.

8.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices and personal devices which connect to the school infrastructure/network *(delete as appropriate)*. This is achieved by:
    - this will be achieved e.g. physical monitoring (supervision), monitoring internet and web access.
- If a concern is identified via monitoring approaches we will:
    - DSL or deputies will respond in line with the child protection policy.
- 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.

8.4 Managing Personal Data Online

 Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. ○ Full information can be found in our Data Protection and Information Security Policy.

8.5 Security and Management of Information Systems

- We adhere to and meet the DfE cybersecurity standards
- We take appropriate steps to ensure the security of our information systems. Further information is available in the DfE cybersecurity standards https://www.gov.uk/guidance/meeting-digital-and-technology-standards-inschools-and-colleges/cyber-security-standards-for-schools-and-colleges ○ Protecting all devices on every network with a properly configured boundary or software firewall
    - Keeping an up-to-date list of every device that is able to access the network and ensuring their security features are enabled, correctly configured and up to date
    - Ensuring that accounts only have the access that they require to perform their role and should be authenticated to access data and services
    - 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 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, ○ The appropriate use of user logins and passwords to access our network.
  - Specific user logins and passwords will be enforced for all but the youngest users.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found at:
- Acceptable use policy

8.5.1 Password Policy

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

- From year 1, all learners are provided with their own unique username and private passwords to access our systems; learners 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.
  - Use two-factor/two-step verification for all accounts which have access to personal or sensitive operational data and functions

8.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (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 our setting 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.

8.7 Publishing Images and Videos Online

 We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

8.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy. ○ The forwarding of any chain messages/emails is not permitted. ○ Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.

- Members of the community will immediately inform Headteacher Charlie Lindsay if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted.

8.8.1 Staff Email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents. 8.8.2 Learner Email
- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

8.9 Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen

- themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

When planning the use of live stream platforms within remote learning our school will:

- Consider whether the technology is available to children/families and make alternative arrangements for provision where necessary.
- Ensure that staff are trained to use the technology.
- Ensure that children's behaviour/interactions are managed in line with the expectations of the school behaviour policy.
- Risk assess the platform being used and consider whether there are functions, such as live chat, pupil's use of video camera, or the recording of the session, which need to be disabled or which require further measures to support their appropriate use.

The above points are relevant to live stream in its broadest sense. What follows next is more relevant, but not exclusively, to the use of platforms allowing twoway video interaction between all users.

- Two members of staff will be 'within the room' when conducting a live stream session with pupils. If the session is being run from school and both adults are there, then they can be physically within the same room. If one or both adults are working remotely then this means that two adults will need to be present within the video call, and they should both be there before the pupils dial in.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or recording features if these cannot be disabled.

- It is the responsibility of the staff member to act as a moderator, raising any issues of suitability (dress, setting, behaviour etc.) with the child and/or parent immediately and ending the online interaction if necessary.
- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering

issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.

- Staff will use school devices and school contact numbers/emails for communications and running the session.
- Only live streaming platforms approved by SLT will be used.
- Staff will dress professionally and choose a neutral background for their video stream.
- Pupils should be dressed appropriately e.g. clothes they might wear for a nonuniform day, not pyjamas.
- Pupils should live stream from a suitable location within their household, not bedrooms.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- All other school policies/practices should be followed, notably the safeguarding and child protection policy so should there be any welfare concerns about the child these should be brought to the attention of the DSL without delay.

Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, the content will be monitored by a member of staff along with the interactions/behaviour of the learners taking part.
- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and then, monitor some sessions to check they are in accordance with the policy.

- We are aware that our filtering and monitoring systems may not necessarily prevent inappropriate content from being shared in a live-streamed event as this is happening in real-time.

Using video calls for 1:1 sessions with children

- The school may consider using 1:1 video call sessions to support interventions with children such as mental health support or counselling.
- These sessions will only be provided where they have been risk assessed and approved by SLT and parental consent given.
- Where the communication with an individual child does not require the confidentiality of a counselling session, there will be two adults involved; this will provide a safeguard for the adults and the children.
- These two adults will either be physically in the same room, with the second member of staff being referenced to the child so that they are aware, or, where staff are working remotely, they will both be within the virtual room of the meeting.
- In either case both adults will be present before the child is admitted to the online session.

8.11 Management of Applications (apps) used to Record Children's Progress (if used)

- We use FFT to track learners progress and share appropriate information with parents and carers.
- The headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:

- Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.

  Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

9. Social Media

9.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of our community.
- 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 our community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of our 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 or that could damage the reputation of the school or individual within it.

- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
    - The use of social media during setting hours for personal use is permitted.

- Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.

- Concerns regarding the online conduct of any member of our community on social media, should be reported to the DSL (or deputy) and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

9.2 Staff Personal Use of Social Media

- 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 Code of Conduct/ Staff behaviour policy as part of Acceptable Use Policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- 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 and using two factor authentication wherever possible.
  - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of our setting on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- 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 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 the 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

- Communication with children both in the offline world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web

- cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour'.
- Staff should not give out any personal contact details.
- On school trips, staff should have a school mobile phone rather than having to rely on their own device.
- Staff should not accept friend requests from pupils, past or present. If a member of staff feels that this is necessary, they should first seek guidance from the DSL or a senior leader. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Headteacher .(See Staff Behaviour Policy/ Code of Conduct for further information).
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher/manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

9.3 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.

- We are aware that many popular social media sites state that they are not for children under the age of 13 (or 16 for WhatsApp), therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and

the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.

- 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 and two factor authentication where possible.
    - 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 setting and externally.
    - To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

9.4 Official Use of Social Media (Only include if setting has official social media)

- Our official social media channels are:
    - List details e.g. twitter link; Facebook page link; YouTube channel link.
- 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 Headteacher.
    - 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.
    - Staff use setting provided email addresses to register for and manage any official social media channels.
    - Official social media sites are suitably protected.
    - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including anti-bullying, image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:

- Sign our social media acceptable use policy.
- Always be professional and aware they are an ambassador for the setting.
- Disclose their official role / position but make it clear that they do not necessarily speak on behalf of the setting.
- Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
- Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent from both pupils and parents before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

10. Use of Personal Devices and Mobile Phones

We recognise that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

10.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Behaviour, Child Protection and Staff Code of Conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
    - All members of our community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
    - All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

10.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
    - Keep mobile phones and personal devices in a safe and secure place during lesson time.
    - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
    - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled when in the school/setting. ○ Not use personal devices during teaching periods, unless written permission has been given by the Headteacher such as in emergency circumstances.
    - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
    - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies and Headteacher Staff will not use personal devices:
    - To take photos or videos of learners and will only use work-provided equipment for this purpose.
    - Directly with learners and will only use work-provided equipment during lessons or educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy ○ If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

10.3 Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- We expect learners' personal devices and mobile phones to be…
    - Kept in the teachers cupboard and switched off
    - Use of 3G, 4G or 5G networks are not permitted in our setting, learners must ensure that mobile data/data roaming is disabled.
- Parents are advised to contact their child via the setting office.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculumbased activity with consent from a member of staff.
- The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the leadership Team.
- Mobile phones and personal devices (including smart watches) must not be taken into examinations / tests.
- Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).

- Searches of mobile phone or personal devices will only be carried out in accordance with our policy. www.gov.uk/government/publications/searchingscreening-and-confiscation)
- Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation)
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

10.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or Headteacher of any breaches our policy.

10.5 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners/parents/carers is required.

- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed of used by members of staff

11. Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies

Useful Links for Educational Settings

East Sussex Support and Guidance:

- East Sussex County Council Early Years Support & Intervention Team ○ Call: 01323 463026
  ○ Email: childcare.support@eastsussex.gov.uk

- If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on 01323 464222 or 0-19.SPOA@eastsussex.gov.uk Standards and Learning Effectiveness Service (SLES): SLES.Safeguarding@eastsussex.gov.uk

East Sussex Support and Guidance for Educational Settings
https://czone.eastsussex.gov.uk/safeguarding/

East Sussex Safeguarding Children Partnership
www.sussexchildprotection.procedures.org.uk/

Sussex Police:

- www.sussex.police.uk

For non-urgent Police contact 101.

If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

 CEOP:

- www.thinkuknow.co.uk
- www.ceop.police.uk

- Childnet: www.childnet.com
  - https://www.childnet.com/what-we-do/our-projects/thrive-online/
  - https://www.childnet.com/resources/connect-with-respect-send/
- Project Evolve: https://projectevolve.co.uk/
- 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: Net-Aware
- 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
- Get Safe Online: www.getsafeonline.org
- Action Fraud: www.actionfraud.police.uk
- Online Safety Toolkit: Online Safety - Czone (eastsussex.gov.uk)

12. Linking your Online Safety Policy with other school policies.

This online safety policy provides educational settings with a framework to develop their online safety ethos and enables leaders and managers to detail strategic approaches and considerations, with regards to the safer use of technology. The

policy should be used as part of an effective whole school approach to online safety. All staff in schools need to understand their responsibilities to ensure that children and young people are able to use the internet appropriately and safely. Schools should ensure online safety is a running and interrelated theme whilst implementing this policy.

The online safety policy should be recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the Designated Safeguarding Lead (DSL).

There is no requirement for educational settings to have a separate online safety policy if online safety issues are appropriately addressed within other policies; this decision will be down to leaders and managers. If online safety is embedded within existing documents, settings should ensure that their community is aware of how and where to locate safety information, especially regarding responding to and reporting specific online safety concerns. As part of the whole school approach safeguarding this policy should link with other relevant policies such as the Child Protection and Safeguarding policy, Behaviour policy, Staff Code of Conduct and Anti-bullying Policy. Schools should also consider whether they need to use Acceptable Use Policies for staff, parents and pupils and how these policies link.

To help you link this policy with your existing Behaviour/Anti-bullying/Acceptable Use Policies please see the table below:

2.0	References the Education and Inspections Act 2006 relating to behaviour outside of school
4.3, 4.6	References Acceptable Use Policies
4.5	References behaviours outside of school
6	References 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
8.1	References behaviour on social media platforms

8.3	References to social media threads and administrators of threads
9.1	References personal mobile devices and possible content that might be offensive, derogatory or would otherwise contravene our behaviour or child protection policies
11.5	References the school's anti-bullying policy
11.7	References how online hate will be responded to in line with existing policies, including anti-bullying and behaviour.

We encourage all educational settings to ensure that their online safety policy is individualised for their own specific context, to ensure that it is fit for purpose. It will not be appropriate for educational settings to adopt this template in its entirety; some statements will be more relevant to some settings than others.

This policy template requires leaders, managers and DSLs to adapt the content to include specific local information such as their own named points of contact, as well as their specific procedures and expectations. These decisions and details will vary from school to school, so this template should be used as a starting framework.

13. Disclaimer

Pupil Acceptable Use of Technology Policy Agreements (including Remote Learning if needed)

We encourage professionals to use these agreements to talk through expected behaviours with their pupils at the start of each term either in form times/PSHE

lessons or IT lessons whether schools are remote learning or not. If your setting is not using live streaming or recording video lessons some statements will need to be deleted/amended as appropriate. Please note, if settings are recording any sessions of remote learning, consent is required from all those involved. Settings should be clear about how recordings will be stored, how long they will be kept for and who will have access to them, in line with your existing Data Protection policy. A template letter and agreement for parents/carers of younger pupils is also included along with reply slips for pupils and parents to fill in. Some settings may find that inputting these statements into online forms such as Google Forms is a more efficient way of having these signed and returned.

Early Year and Key Stage 1 (0-6)

The Agreement

This agreement is intended to help our younger pupils understand:

- How to stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- That they must use school systems in a responsible way, to ensure that there is no risk to their own safety or to the safety and security of the systems and other users.

This is how we stay safe when we use computers at school and at home:

- I will ask an adult if I want to use the computers / devices and will only use it when they are with me;
- I will only use activities that an adult has told or allowed me to use;
- I will keep information about me safe;
- I will not share my password;
- I will be kind to others online when I am sending messages;

- I will ask for help from an adult if I am not sure what to do or if I think something has gone wrong;
- I will tell an adult if I see something that upsets me on the screen or if I am worried or unsure;
- I know that if I don't follow these rules I might not be allowed to use the computers / devices;

When I am learning from home:

- I will ask an adult if I want to use a computer or device;
- If I am in a 'live lesson' with my teacher an adult will be close by me;
- I will make sure that I use my computer or device in a shared space, (not in my bedroom);
- I will only do activities online that a teacher or suitable adult has told me or allowed me to use;
- I will ask for help from an adult if I am not sure what to do or if I think something has gone wrong;
- I will tell a teacher or adult if I see something that upsets me on the screen or if I am worried or unsure about something;

Childs Name:

Class:

Date:

Parents Name:

Parents Signature:

Date:

Key Stage 2 (7-11)

The Agreement

This Acceptable Use Policy Agreement is intended to ensure:

- that pupils at the school/setting will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

I understand that I must use school devices and systems in a responsible way and that this agreement will keep me safe when I am online at home and at school.

For my own personal safety:

- I know that I will be able to use the internet in school/setting for many different activities and to keep myself and others safe I must use it responsibly.
- I will not share my password with anyone, and I will log off when I have finished using the computer or device.
- I will protect myself by not telling anyone I meet online any of my personal information. This includes my address, my telephone number, my school/setting name.
- I will not send a picture of myself without permission from a teacher or other adult.
- I will not arrange to meet anyone I have met online alone in person without talking to a trusted adult.
- I will tell a teacher or other adult if someone online makes me feel uncomfortable or worried when I am online using games or other websites or apps.

I understand that everyone has equal rights to use technology as a resource and:

- I know that posting anonymous messages or pretending to be someone else is not allowed.
- I know that information on the internet may not be reliable and it sometimes needs checking so I will not download any material from the internet unless I have permission.
- I know that memory sticks/CDs from outside of the school may carry viruses so I will always give them to my teacher so they can be checked before opening them.
- I know that I am not allowed on personal email, social networking sites or instant messaging in school/setting
- I know that all school/setting devices/computers and systems are filtered and monitored, including when I am using them at home.

I will act as I expect others to act toward me and:

- I will be polite and sensible when I message people online I will not be rude or hurt someone's feelings online.
- I will not purposely exclude others from online activities
- I will not look for bad language, inappropriate images or violent or unsuitable games or content, and if I accidently come across any of these, I will report it to a teacher or adult in school/setting, or a parent/carer at home.
- If I get unkind, rude, or bullying emails or messages, I will report them to a teacher/adult. I will not delete them; I will show them to the adult so that they can help me.

When working from home (remote learning):

These expectations are in place to help keep me safe when I am learning at home using system name e.g. Microsoft Teams, Google Meet etc.

- When taking part in a live lesson I understand that I must take part from somewhere appropriate at home (not in my bedroom) with limited distractions and I must wear appropriate clothing;

- I understand that my teachers may mute my microphone and I should wait for them to unmute it rather than unmuting it myself;
- I understand that I should only communicate with my teacher through prearranged live lessons or using school email;
- I will not record teacher audio or video presentations, nor will I take screenshots or photos of teachers or other pupils or anyone else involved in a live lesson;
- I will not share or distribute any of the teacher presentations and online teaching resources;
- I will not change or edit of any of the teaching resources made available except for my own personal use;
- I will not take, use, share, publish or distribute images of others without their permission;
- I will not share any access links to these remote learning sessions with others;
- I understand that I must behave online as I would in a classroom;
- I will only use the chat feature for work related discussions;
- I have read and talked about these rules with my parents/carers;
- I understand that if I do not follow this agreement, I may not be allowed to use the internet at school/setting.

Childs Name:

Childs Signature:

Class:

Date:

Parents Name:

Parents Signature:

Date:

Key Stage 3/4/5 (11-18)

The Agreement

I understand that the school/setting Acceptable Use Policy Agreement will help keep me safe online at home and at school.

This Acceptable Use Agreement is intended to ensure:

- that all pupils at the school/setting will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and the safety of those using them at risk. Pupils will have good access to digital technologies to enhance their learning and school/setting will, in return, expect the pupils to agree to be responsible users.

For my own personal safety:

- I understand that the school/setting will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of the risks of communicating with others online, and in particular those who I have only met online.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- I understand the risks associated with meeting someone offline that I have only communicated with online and will not do this without speaking to a trusted adult. In the unlikely event that I have arranged to meet people off-line that I have communicated with on-line, I will do so in a public place and take an

adult with me. (school/setting does not recommend any pupil arranging to meet people in this way unless as part of an educational visit with an authorised member of staff e.g. Digital Leaders Scheme)

- I will immediately report any unpleasant, offensive or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.
- I understand that the school/setting internet filter is there to protect me, and I will not try to bypass it.
- I will make sure that my internet use is safe and legal, and I am aware that online actions have offline consequences.
- I know I must always check my privacy settings are safe and private.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school/setting and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school/setting systems or devices for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me and:

- I will not access or change other people files, accounts, or information.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

- I know that bullying in any form (on and offline) is not tolerated and I know that technology should not be used for harassment.
- I will not take or distribute images of anyone without their permission.
- I will write emails and online messages carefully and politely as I know they could be forwarded or seen by someone I did not intend.
- I understand that it may be a criminal offence or breach of the school/setting policy to download or share inappropriate pictures, videos, or other material online. I also understand that it is against the law to take, receive, save or send indecent images of anyone under the age of 18.
- I will always think before I post, I know that text, photos or videos can become public and very difficult and sometimes impossible to delete.

I understand that the school/setting **has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.**

- I will not use my own personal devices (mobile phones / USB devices etc) in school unless this is specifically allowed (e.g. BYOD).
- I understand the risks and will not try to upload, download or access any materials which are illegal, offensive or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software; however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes). Even if I know the sender, I will take care and not click on any links if something looks suspicious.
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer/device settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- If I am making use of AI technology (e.g. ChatGPT) I will clearly reference where the content came from and where/how it was created.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school/setting also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community, e.g. if my behaviour online poses a threat or causes harm to another pupil and/or could have repercussions for the orderly running of the school then I understand that the school can take action against me.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action in line with the school's behaviour policy. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Remote Learning

These expectations are in place to help keep me safe when I am learning at home using system name e.g. Microsoft Teams, Google Meet etc.

- When taking part in a live lesson I understand that I must take part in lessons from somewhere appropriate at home (not in my bedroom) with limited distractions and I must wear appropriate clothing;
- I will ensure backgrounds of videos are neutral/blurred and personal information/content is not visible;
- I will attend lessons in a shared/communal space or room with an open door and/or where possible when I can be supervised by a parent/carer or another appropriate adult.
- I understand that my teachers may mute my microphone and I should wait for them to unmute it rather than unmuting it myself;
- I understand that I should communicate with my teacher through prearranged live lessons or using school email;
- I will not record teacher audio or video presentations, nor will I take screenshots or photos of teachers, other pupils or anyone else taking part in a live lesson;
- I will not share or distribute any of the teacher presentations and online teaching resources;
- I will not edit of any of the teaching resources made available except for my own personal use;
- I will not take, use, share, publish or distribute images of others without their permission;
- I will not share any access links to these remote learning sessions with others;
- If I am concerned about anything that takes place during remote learning, I will inform a suitable adult;
- I understand that I must behave online as I would in a classroom.
- I understand that inappropriate online behaviour or concerns about my safety during remote learning will be taken seriously. This could include not being able to access these lessons, parents/carers being informed or contact with the police if a criminal offence has been committed;
- I will only use the chat feature for work related discussion
- I have read and talked about these rules with my parents/carers.

Key Stage 3/4/5 Acceptable Use Agreement Form

This form relates to the Pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school/setting systems and devices (both in and out of school)
- I use my own devices in the school/setting (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment outside of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc. or in a way that could disrupt the orderly running of the school.

Childs Name:

Childs Signature:

Class:

Date:

Parents Name:

Parents Signature:

Date:

Template letter to Parents/carers for Early Years – Key Stage 1 Children

This letter can be amended to use with older children.

Dear Parents and Guardians,

As part of their learning and development, your child will have the opportunity to access a wide range of digital technologies, including computers, games and i-pads at school. We recognise the value of using these digital technologies and the potential risks involved and therefore have rigorous online safety policies and procedures in place which are available to read on our website.

During a time of Remote Home Learning your child will also have the opportunity to access digital technology at home, as they do at school. We recognise the value of using these digital technologies, but also the potential risks involved.

In order to support us further in developing your child's knowledge and understanding about online safety, please read the agreement below and discuss this with your child. We then ask that you sign and return the slip below. We understand that your child is too young to give informed consent on their own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful partnership.

Hopefully, you will also find these rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the online and digital technologies, both within and beyond the early years setting environment, such as at home or at a friend's home.

Signed by DSL/Head etc

Acceptable Use of Technology Template Statement and Forms for Parents/Carers

These statements need to be amended according to online policies, mobile use policies, social media policies and any remote provision within each setting.

- I have read – and discussed with my child the pupil Acceptable Use of Technology Agreement Policy (AUP) for school/setting and understand that this AUP will help keep my child safe online;
- I understand that the AUP applies to my child's use of school/setting devices and systems on site and at home, and personal use where there are safeguarding and/or behaviour concerns;
- I am aware that the use of school/setting devices and systems may be monitored for safety and security reason to keep my child safe. This monitoring will take place in accordance with data protection, privacy, and human rights legislation and further information about the school's approach can be found
- I understand that my child needs a safe and appropriate place to access remote learning if school/setting is closed in response to Covid-19 or if my child needs to self-isolate at home. I will ensure my child's access to remote learning is appropriately supervised. When accessing video learning, I will ensure they are in an appropriate location (e.g. not in a bedroom) and that they are suitably dressed
- I give permission for my child/ren to access system name e.g. Microsoft Teams, Google Meet etc
- I give permission for my child to participate in live lessons with their form teacher and subject teachers; (delete if this is not appropriate)
- I understand that I will be asked for permission by the subject teacher (via email) if my child needs a 1:1 live lesson (e.g. for Learning Support, EAL etc.);
- I understand that any 1:1 live lessons will be recorded and saved on the school/setting server and kept in accordance with data protection;

- I give permission for my child to submit work and upload work related videos to their teacher;
- I understand that the school/setting will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use school/setting devices and systems. I understand that the school/setting cannot ultimately be held responsible for the nature and content of materials accessed on the internet or if my child is using their own mobile technologies
- I give permission for my child's work to be used on school/setting Social Media Account;
- I 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/setting community.
- I understand that the school/setting will contact me if they have concerns about any possible breaches of the AUP or have any concerns about my child's safety.
- I will inform the school/setting or other relevant organisations if I have concerns over my child's or other members of the school/setting communities' safety online.
- I understand that if my child fails to comply with this Acceptable Use Policy Agreement, they may be subject to disciplinary action in line with the school's behaviour policy. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- 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/setting.
- I will support the school/setting online safety approaches and will discuss this agreement and the pupil agreement with my child. I will use appropriate parental controls and will encourage my child to adopt safe use of the internet and other technology at home, as appropriate to their age and understanding.

I understand that I must have returned this Consent for Remote Learning Form before my child can take part in any Remote Learning.

Childs Name:

Class:

Date:

Parents Name:

Parents Signature:

Date:

Staff Remote Learning AUP

This Remote Learning Acceptable Use Agreement Policy is intended to ensure:

- that staff and volunteers at school/setting will be responsible users and stay safe while using the internet and other communications technologies whilst remotely teaching pupils who are not in school.
- that school/setting users are protected from accidental or deliberate misuse that could put users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

School/setting will try to ensure that staff and volunteers have good access to digital technology and training to enhance their work, to enhance learning opportunities for pupils' learning and will, in return, expect staff and volunteers to agree to be responsible users.

This Policy should be read alongside the school/setting Staff (and Volunteer) Acceptable Use Agreement and Remote Learning Policy/Online Policy.

I understand that I must use school/setting systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

- I will be aware of and understand my responsibilities when delivering remote lessons.

- I understand that communication with children both off and online must take place within explicit professional boundaries.

  I will be aware of the following policies and procedures:

  - Safeguarding and Child Protection Policy
  - Online Policy and Staff Acceptable Use Policy
  - Behaviour policy
  - Staff Code of Conduct
  - Social Media Policy
  - Policy for the Prevention of Bullying (Amend accordingly)

- I will not use any personal accounts to communicate with pupils and/or parents/carers
- I will not seek to communicate/make contact or respond to contact with pupils outside of the purposes of my work or outside of school hours;
- I will use work provided equipment where possible e.g., a school/setting laptop, tablet, or other mobile device – where not possible clear expectations in need to be place in relation to safeguarding and data security when using personal devices e.g., using strong passwords, suitable levels of encryption, logging off when not in use etc.
- I am aware that online bullying is a safeguarding issue and that any incidents of this must be reported to the DSL as per school/setting Safeguarding procedures.
- I will report any suspected misuse or problem to the Online Safety Coordinator (DSL) or Network Manager for investigation / action / sanction
- If I am a Form /Class teacher, I will ensure all my pupils have understood and returned the Pupil Remote Learning Home Agreement;
- If I am a Form /Class teacher, I will provide remote pastoral care for my class;
- I will continue to look out for signs that a child may be at risk whilst teaching remotely;

- I understand that it is best practice that staff will guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. e.g. Google Images.

- I will be mindful of the added pressure that remote learning can add to any household and, in particular, in a household with more vulnerable children,
- If I am a SEN or EAL teacher, I will provide assistance to teachers who require help to differentiate and will ensure contact with pupils and their parents who are likely to require further assistance.
- If I am a Form /Class teacher, I will ensure I have regular contact with my class;
- I will make contact with pupils only via school/setting provided email accounts or logins.
- When recording videos and for live lessons I understand that I must wear appropriate clothing
- I understand that for live lessons at least 2 members of staff should be present and where this is not possible the leadership team approval will be sought. I understand that live lessons should be recorded and backed up on Teams Streams/school server, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.
- I understand that any 1-1 live lessons need to be pre-arranged, with written parental consent given and that two adults need to be present. Where 1-1 sessions may be necessary these sessions must be recorded and saved to the school server where this can be reviewed at any time.
- I will not record lessons or meetings using personal equipment.
- I understand that any computers used for such recordings or live lessons should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral/blurred background.
- I understand that live lessons should be recorded and backed up on Teams Streams/school server, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.

- I understand that all my language must be professional and appropriate, including if any of my family members are in the background;
- I will not give out my personal details;
  I will not take images of pupils for my own personal use;
- I will not display or distribute images of pupils unless they have parental consent to do so (and, where appropriate, consent from the child)
- At the beginning of each session I will remind pupils of behaviour expectations and reporting mechanisms at the start of the session, including the use of microphones and chat features.
- I will remind pupils to report concerns during remote and/or live streamed sessions:
- If inappropriate language or behaviour takes place, pupils involved will be removed by staff, and concerns will be reported to name/role
- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, antibullying and behaviour.
- I will report any safeguarding concerns will be reported to school/setting Designated Safeguarding Lead, in line with our child protection policy.

I have read and understood the Remote Learning Acceptable Use Policy (AUP) for staff.

Name:

Date:

Online Policy Annex – school/setting **Remote Learning/Meeting Policy**

This policy should be read alongside the school/setting Online Policy, which also incorporates the acceptable use of technologies, staff, pupil and parent relationships/conduct and communication.

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. At school/setting we believe in teaching our pupils about Digital Resilience and the education of pupils in online safety is therefore an essential part of our school's online safety provision. Children and young people need the help and support of the school and their parents/carers to recognise and avoid online safety risks and build their resilience.

Please refer to our Online Policy for further information on Roles and Responsibilities, Education, Data Protection and Technical Infrastructures (Amend as necessary)

Policy Aims:

- To provide and deliver an enriching curriculum remotely
- To do so safely and with consideration of online dangers
- To continue to promote good relationships and conduct between all members of the school community.

General Expectations for All Staff and Governors

- All staff must be aware of and understand their responsibilities when delivering remote lessons
- All staff must be aware of the following policies and procedures:

- Safeguarding and Child Protection Policy
- Online Policy and Staff Acceptable Use Policy
- Behaviour policy
- Staff Code of Conduct
- Social Media Policy
- Policy for the Prevention of Bullying
- (amend all as necessary)

- The name and role will ensure that staff know the expectations for virtual learning and provide training for staff with video tutorials to ensure that good quality provision is provided.
- The name and role will assist staff with any technological problems and further training.
- The DSL name and role will identify any safeguarding concerns raised through MyConcern/CPOMS/Amend regarding staff or pupils and act accordingly as per normal procedures.
- The DSL will provide a list of pupils considered vulnerable to help inform the actions of staff who are offering remote pastoral care, relevant staff will be in regular contact with those pupils.
- Staff are aware that online bullying is a safeguarding issue and that any incidents of this must be reported to the DSL as per school/setting Safeguarding procedures.
- Staff will report any safeguarding concern to the DSL MyConcern/CPOMS/Amend.
- Staff will report any suspected misuse or problem to the Online Safety Coordinator (DSL) or name and role for investigation / action / sanction
- Staff will ensure all their pupils and parents have understood and returned the Pupil/Parent Acceptable Use Policy Agreements.
- Staff will provide remote pastoral care, passing on any academic or pastoral matters as necessary to the name and role
- Staff will make provisions for those families who have limited facilities or resources to access the remote learning.

- It is best practice that staff will guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. e.g. Google Images.
- All staff will be mindful of the added pressure that remote learning can add to any household and, in particular, in a household with more vulnerable children.
- SEN teachers will provide assistance to teachers who require help to differentiate and will ensure contact with pupils and their parents who are likely to require further assistance.
- This also applies to EAL staff.
- Form/class teachers will make regular contact with their pupils and parents via school email accounts/logins or where necessary by phone.
- All remote learning and any other online communication will take place in line with current school/setting confidentiality expectations;
- Appropriate privacy and safety settings will be used to manage access and interactions. Place detail here on the specifics according to the system being used e.g. language filters, limiting chat, staff not permitting learners to share screens, keeping meeting IDs private, use of waiting lobbies or equivalent.
- 1-1 Live Lessons need to be pre-arranged, with written parental consent given and 2 adults need to be present. Where these sessions may be necessary, they must be recorded and saved to Teams Streams/School server/Amend where this can be reviewed at any time.
- When recording videos and for Live Lessons staff must wear appropriate clothing.
- Any computers used for such recordings or Live lessons should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral/blurred background.
- Live Clinics should be recorded and backed up on Teams Streams/school server/amend, so that if any issues were to arise, the video can be reviewed.
- Language must be professional and appropriate, including any family members in the background

Responsibilities of Parents and Pupils for Live Lessons/meetings with school staff:

- Parents must have understood and returned the Consent for Remote Learning Form/AUP before they can take part in a virtual lesson/live session.
- A pre-agreed invitation/email/ detailing the session expectations will be sent to those invited to attend.
- Pupils must take part in the lesson from somewhere appropriate at home with limited distractions and in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer.
- Pupils should only communicate with the teacher through pre-arranged live lessons or via school email and ideally parents should be copied into this correspondence.
- Pupils can have their microphones muted by a member of staff and should wait for the teacher to unmute them rather than unmuting themselves.
- Pupils must not record teacher audio or video presentations or take screenshots or photos of teachers and other students
- Pupils must not share or distribute any of the teacher presentations and online teaching resources
- Pupils must not edit of any of the teaching resources made available except for their own personal use
- Breach of any of the above could result in removal from the lesson, access to online content removed and an appropriate sanction set in line with the Behaviour for learning policy
- Pupils must behave online as they would in their classrooms. In the event of a teacher deeming any behaviour inappropriate they reserve the right to remove the pupil from the lesson and give drills as per our usual behaviour policy.
- Pupils and Parents must be aware that school/setting takes online bullying very seriously and will respond as per our Policy for the Prevention of Bullying to any incidents of this nature.

- Parents must be aware that there are lots of people offering support to parents for home schooling via groups and live streams across a multitude of platforms. This unfortunately could be seen as an opportunity for unsavoury characters to find their way to young people.
- Alternative approaches and/or access will be provided to those who do not have access.

Meeting digital technology standards in schools

Filtering and monitoring standards

Task/responsibility	**Notes**
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	
Responsibility: Gov **Task:** Identify and assign a member of the SLT to be responsible for ensuring that the standards are met	Hayley Cross - Safeguarding Governor Kate Tugwell - SLT
Responsibility: Gov **Task**: Identify and assign a governor to be responsible for ensuring that the standards are met	Hayley Cross - Safeguarding Governor
Responsibility: Gov **Task**: Identify and assign the roles and Headteacher responsibilities of staff and third parties (incl. external service providers)	Hayley Cross - Safeguarding Governor Headteacher - Charlie Lindsay Deputy Headteacher - Kate Tugwell
Responsibility: Gov **Task**: Is it possible to make "prompt" changes to provision?	Hayley Cross - Safeguarding Governor Yes - termly meetings with DSL Kate Tugwell to oversee chamges made eg Individual passwords for EYFS introduced December 2023

Responsibility: SLT with support from DSL and ITSP **Task**: Procuring filtering and monitoring	DSL Kate Tugwell Schools ICT - It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. Company / Organisation Smoothwall (part of Qoria) Address Second Floor, 2 Whitehall Quay, Leeds, LS1 4HR Contact details https://www.smoothwall.com/education/contact-us/ Filtering System Smoothwall Filter Date of assessment 30/08/2023

systems	
Responsibility: SLT **Task**: Document decisions about what is blocked or allowed and why	Local Authority / SMOOTHWALL ESCC - Blocked Categories , Smoothwall Filter provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and "Non-Pornographic Nudity" through to "News", "Sport" and "Online Games".
Responsibility: SLT **Task**: Review the effectiveness of your provision (and provide evidence)	Daily data breach reports generated by Smoothwall Termly reporting of Online Safety breaches to governors by DSL Kate Tugwell. Shared with Safeguarding governor at termly visit.
Responsibility: SLT **Task**: Oversee reports	Yes - School Business manager and DSL review reports
Responsibility: SLT **Task**: All staff have received appropriate and up to date	Yes - all staff have completed online safety training and annual updates using Educare. ..\..\..\Staff\Online Training.xlsx

training and understand their role	
Responsibility: SLT **Task**: All staff follow policies and procedures and processes around online safety and filtering and monitoring	Yes - all staff must read and sign off that they have read the Online Safety Policy. Staff meeting updates provided by DSL Kate Tugwell relating to filtering and monitoring (see staff training powerpoint.)
Responsibility: SLT **Task**: All staff act on reports and concerns	Yes - reported on My Concern following the safeguarding policy.
Responsibility: DSL **Task**: Oversee and act on filtering and monitoring reports	Yes
Responsibility: DSL **Task**: Oversee and act on safeguarding concerns	Yes - in line with all Safeguarding Concerns reported. Where relevant, concerns reviewed in weekly welfare meeting.
Responsibility: DSL	Kate Tugwell
Task: Oversee and act on checks to monitoring systems	Yes - DSL receives daily data breach reports and acts on any concerns - generally by speaking to relevant staff.
Responsibility: ITSP **Task**: Maintain filtering and monitoring systems	Smoothwall Filter offers a wide range of techniques for identifying users – including negotiate authentication, login pages and RADIUS compatibility, as well as a number of custom options.
Responsibility: ITSP	Daily data breach reports generated

Task: Provide filtering and monitoring reports	Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device. Logs are retained to customer preference.
Responsibility: ITSP **Task**: Complete actions following concerns or checks to systems	Smoothwall Filter offers a wide range of techniques for identifying users – including negotiate authentication, login pages and RADIUS compatibility, as well as a number of custom options. Where it is possible and clear to pinpoint the exact child / device, DSL will speak to the child / teacher / parent.

Task/responsibility	**Notes**
You should review your filtering and monitoring provision at least annually	
Responsibility: Joint **Task**: Carry out reviews of the filtering and monitoring provision at least annually	Yes - this is managed centrally by SCHOOLS ICT.
Responsibility: Joint **Task**: Carry out checks which are informed by the review to ensure systems are working	To be carried out by DSL Kate Tugwell using www.testfiltering.com 08.01.2024
Responsibility: Joint **Task**: Understand the risk profile of pupils – incl. those in vulnerable groups, age, SEND, EAL	Smoothwall Filter integrates with a wide variety of directories (e.g. Microsoft AD, Azure AD, Google Directory) allowing filtering to be set appropriately at group and user level. It is also possible to combine user group with location (eg outside school)
Responsibility: Joint **Task**: What does the filtering system block/allow and why?	Smoothwall - The 'Intolerance' category covers any sites which promote racial hatred, homophobia or persecution of minorities. Sites which advocate violence against these groups are also covered by the Violence category. Drugs /

	Substance abuse displays or promotes the illegal use of drugs or substances The Drugs category covers the sale, manufacture, promotion or use of recreational drugs as well as abuse of prescription drugs. Sites which provide resources which aim to help those suffering from substance abuse are covered by the 'Medical Information' category. Sites which discuss Alcohol or Tobacco are covered by the 'Alcohol and Tobacco' category. Extremism promotes terrorism and terrorist ideologies, violence or intolerance The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'. Smoothwall also provides both a 'Violence' category which covers violence against both animals or people; An 'Intolerance' category (covered further above) and a 'Gore' category which covers any sites which describe or display gory images and video. Gambling Enables gambling The Gambling category includes all online gambling sites, along with sites promoting gambling or discussing strategies for gambling Malware / Hacking promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content As well as providing a level of protection against externally created malware, Smoothwall Filter provides a Hacking category which includes sites such as "how to" on hacking, and sites encouraging malicious computer use. Filter bypass tools

	are covered separately in a comprehensive “web proxies” category, which uses a combination of domain lists and dynamic content analysis. Pornography displays sexual acts or explicit images The ‘Pornography’ category contains sites containing pornographic images, videos and text. Sites which contain mild nudity for purposes other than sexual arousal are covered by the ‘NonPornographic Nudity’ category. The ‘Pornography’ category uses both a list of domains/URLs as well as dynamic content rules which ensure new, previously unseen sites can be identified on the fly. Piracy and copyright theft includes illegal provision of copyrighted material The ‘Piracy and Copyright Infringement’ category contains sites which illegally provide copyright material or provide peer-to-peer software. Self Harm promotes or displays deliberate self harm (including suicide and eating disorders) The ‘Self Harm’ category contains sites relating to selfharm, suicide and eating disorders. The category excludes sites which aim to provide medical or charitable assistance which are categorised as ‘Medical Information’ or ‘Charity and Non-Profit’ respectively. Violence Displays or promotes the use of physical force intended to hurt or kill The ‘Violence’ category contains sites which advocate violence against people and animals. We also provide a ‘Gore’ category which contains images and video of gory content.

Responsibility: Joint **Task**: Are there any outside safeguarding	Ensure that this is relevant to your school or setting

influences that should be considered (e.g. county lines)	Yes - county lines is prevelant in our local community with 4 orbital railway stations. We work closely with our local Police Youth Engagement officer, PC Paul Eastes.
Responsibility: Joint **Task**: Are there any relevant safeguarding reports that could/should impact on filtering and monitoring?	MyConcern report monitoring gives guidance on current trends in concerns.
Responsibility: Joint **Task**: How digitally resilient are pupils?	Sandown pupils are highly digitally resilient. They receive lessons every term both explicitly through the Purple mash / Rising Stars online safety curriculum lessons and also through frequent reminders via the wider curriculum.
Responsibility: Joint **Task**: What does the RHSE and PSHE curricula cover and how might this impact on filtering?	Our preventative curriculum is carefully crafted to ensure pupils learn and know how to keep themselves safe online. Certain topics in RSE and PSHE causes data breaches eg drugs / self harm / suicide / alcohol and tobacco and healthy relationships.
Responsibility: Joint **Task**: How are devices used within school? (e.g. BYOD)	All devices used at school devices. Children are not permitted to bring any devices into school. No smart watches are permitted either. Any phones are switched off and kept locked away during the school day.

Responsibility: Joint **Task**: What related safeguarding and technology policies are in place?	Safeguarding policy RSE policy Online Safety Policy Staff Code of Conduct AUP
Responsibility: Joint **Task**: What checks are in place – how are resulting actions handled? *Checks should be undertaken from a safeguarding **and** an IT perspective*	DSL and School Business Manager monitor daily Smoothwall . Resulting actions are addressed by DSL by speaking to relevant staff / pupils / parents in line with Safeguarding Policy.
Responsibility: Joint **Task**: How often are checks carried out, what is checked? *Filtering should be tested – log what is done and the results that are obtained – make changes as a result. Different devices should be used when carrying out checks in order to get a good overview of what is or is not*	Annually by DSL Resulting test results reviewed with Safeguarding Governor and any changes decided with support from Schools ICT.
accessible.	
Responsibility: Joint **Task**: How does monitoring work? *How often are reports received – are these in real time – what thresholds are in place – are these fit for purpose?*	Smoothwall data breach reports generated daily and sent to DSL and School Business manager. Reports are in real time.

Responsibility: Joint **Task**: Does filtering and monitoring work on new devices? Is this checked before they are given to staff/pupils?	Smoothwall Filter offers both network level filtering, and device based filtering, for use as appropriate. Smoothwall is applied to ALL devices in the school and the school wifi.
Responsibility: Joint **Task**: Review blocklists and modify in line with any changes to safeguarding risks	Smoothwall maintains a "blocklist policy document" which includes clear criteria on what should and should not be in each category.
Responsibility: Joint **Task**: Check your system using the SWGfL testing tool to see that it is blocking access to illegal child sexual abuse material, unlawful terrorist content, adult content	Yes

Task/responsibility	**Notes**
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	
Responsibility: DSL and ITSP **Task**: Is your filtering provider a member of the IWF?	Yes, Smoothwall is a member of the Internet Watch Foundation and implements the IWF CAIC list.

Responsibility: DSL and ITSP **Task**: Does your filtering provider use the IWF list?	Smoothwall implements the IWF CAIC list of domains and URLs. Smoothwall Filter also uses a number of search terms and phrases provided by IWF and their members. We perform self-certification tests daily to ensure that IWF content is always blocked through a Smoothwall Filter.

Responsibility: DSL and ITSP **Task**: Does your filtering provider use the CTIRU list?	Counter Terrorism Internet referral Unit - Yes Smoothwall Filter implements the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. The 'Terrorism' category contains the 'police assessed list of unlawful terrorist content'.
Responsibility: DSL and ITSP **Task**: Are you blocking access to adult content?	Yes - Smoothwall blocks discrimination, drugs / substance, extremism, gambling, hacking . malware, pornography,self harm, violence As well as the categories listed above, Smoothwall Filter provides filtering and reporting for over 100 other categories ranging from 'Sexuality Sites' and "Non-Pornographic Nudity" through to "News", "Sport" and "Online Games".
Responsibility: DSL and ITSP **Task**: Is filtering applied to all accounts including guest accounts? (Staff, pupils)	Yes - Smoothwall Filter integrates with a wide variety of directories (e.g. Microsoft AD, Azure AD, Google Directory) allowing filtering to be set appropriately at group and user level. It is also possible to combine user group with location (eg outside school)
Responsibility: DSL and ITSP **Task**: Is filtering applied to all school owned devices?	Yes - all devices including laptops and chrome books and iPads
Responsibility: DSL and ITSP **Task**: Is filtering applied to any device which connects to the school broadband connection?	Yes - school wifi system tested by DSL (December 2023) Smoothwall Filter has a full range of policy tools available, allowing School Any changes to

	the filter system are logged enabling an audit trail that ensure transparency and that individuals are not able to make unilateral changes users to easily make policy changes, test a site against current policy or simply quickly allow or block a site
Responsibility: DSL and ITSP **Task**: Do you filter all internet feeds including any backup connection?	Yes
Responsibility: DSL and ITSP **Task**: Is filtering differentiated by age and ability of pupils?	Yes - Smoothwall Filter integrates with a wide variety of directories (e.g. Microsoft AD, Azure AD, Google Directory) allowing filtering to be set appropriately at group and user level. It is also possible to combine user group with location
Responsibility: DSL and ITSP	
Task: Can filtering handle multilingual content, images, misspellings, abbreviations?	Smoothwall's combined blocklist includes words in a wide variety of languages, focussed on those spoken in UK and US schools. This includes Polish and Spanish as well as "non latin" such as Urdu and Russian.
Responsibility: DSL and ITSP **Task**: Can filtering identify VPNs and proxy services and then block them?	Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure) Smoothwall Filter offers both network level filtering, and

	device based filtering, for use as appropriate.
Responsibility: DSL and ITSP **Task**: Can filtering system provide alerts when access to content has been blocked?	Yes - Smoothwa;ll reports generated daily. Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device. Logs are retained to customer preference
Responsibility: DSL and ITSP **Task**: Does filtering work on mobile devices? *Is there evidence, have you checked?*	Yes - DSL has checked that the school wifi bloicks access to inappropriate sites using a mobile device. Smoothwall Filter offers both network level filtering, and device based filtering, for use as appropriate.
Responsibility: DSL and ITSP **Task**: Does filtering work on app content? *Is there evidence, have you checked?*	Any app content delivered via HTTPS (not necessarily through a web browser) can be blocked and inspected by Smoothwall's on-premise network appliance, assuming the app permits this. In addition, Smoothwall's optional firewall module can identify and block many other types of app.
Responsibility: DSL and ITSP **Task**: Will the filtering system identify the IP address, device name and ID and where possible the individual who has attempted to access unsuitable or illegal content?	Partially. This is something I have raised repeatedly with Schools ICT and with Smoothwall. Smoothwall claim that 'Smoothwall Filter offers a wide range of techniques for identifying users – including negotiate authentication, login pages and RADIUS compatibility,

	as well as a number of custom options. Smoothwall Filter offers a comprehensive suite of reports and logs, with a complete URL-by-URL record of all web activities including timestamp, username and source device. Logs are retained to customer preference.

Task/responsibility	**Notes**
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	
Responsibility: ITSP **Task**: Are monitoring systems working as expected?	Yes - although we are not always able to identify the exact individual or device specifically.
Responsibility: ITSP **Task**: Are reports on pupil device activity available?	Yes
Responsibility: ITSP **Task**: Are IT staff given safeguarding training including online safety training?	Yes
Responsibility: ITSP **Task**: Are IT staff reporting any issues (safeguarding concerns to the DSL)?	Yes
Responsibility: All staff **Task:** Are the wider staff body reporting safeguarding concerns to the DSL	Yes - via MyConcern in line with all Safeguarding reporting concerns policy.

Responsibility: All staff **Task:** Are the wider staff body providing effective supervision of pupils?	Yes
Responsibility: All staff **Task:** Are the wider staff body taking steps to maintain awareness of how devices are being used by pupils?	Yes - and we have asked for Net Support to be added to all teacher laptops to allow for whole class device monitoring during lessons.

Key:

Gov Governor with designated responsibility for online safety/safeguarding

DSL Designated safeguarding lead

SLT Member of the senior leadership/senior management team

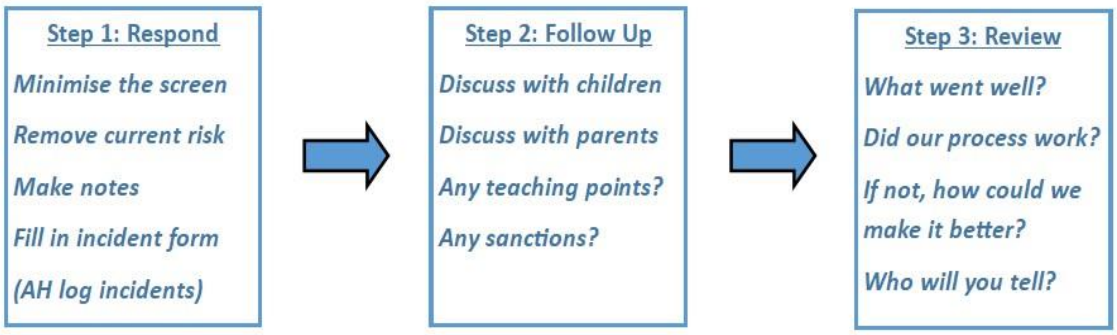
ITSP IT service provider (this may be a staff technician or an external service provider)

JOINT This group should comprise the responsible governor, a member of SLT, the DSL and the IT service provider.

All members of staff who are working with pupils in any capacity.

Online Safety Incidents

To keep children at Sandown safe online, staff follow the three-step plan for any online safety incident.



Children should be taught to immediately tell an adult about anything they see on screen that makes them upset, uncomfortable or worried. They should also sign an Acceptable Usage Policy in which they agree not to access any sites which they know to be banned, or which they know to be inappropriate to access during learning time.