



ONLINE SAFETY POLICY

This Online Safety policy has been developed by an Online Safety Group made up of:

- Head
- DSL
- Network Manager
- Safeguarding Governor

Schedule for Development / Monitoring / Review

The Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>Once a term</i>
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>August 2024</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>LADO, East Sussex Police, CEOP</i>

Contents

Schedule for Development / Monitoring / Review	1
Important information	5
1. Policy Aims	6
2. Policy Scope	7
2.1 Links with other policies and practices	8
2.2 Online safety in community activities, after-school clubs and tuition.....	8
3. Monitoring and Review.....	9
4. Roles and Responsibilities	10
4.1 The leadership and management team and governors will:	10
4.2 The Designated Safeguarding Lead (DSL) will:.....	12
4.3 It is the responsibility of all members of staff to:	13
4.4 It is the responsibility of staff managing the technical environment to:	14
4.5. It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:	14
4.6 It is the responsibility of parents and carers to:	15
5. Education and Engagement Approaches	16
5.1 Education and engagement with pupils.....	16
5.2 Vulnerable Pupils	17

5.3 Training and engagement with staff	17
5.4 Awareness and engagement with parents and carers	18
6. Responding to Online Safety Incidents and Concerns	19
6.1 Concerns about Pupils' Welfare	20
6.2 Staff Misuse	20
7. Procedures for Responding to Specific Online Incidents or Concerns.....	21
7.1 Child-on-child online sexual violence and sexual harassment.....	21
7.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes')	23
7.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines)	25
7.4 Indecent Images of Children (IIOC).....	27
7.5 Cyberbullying	28
7.6 Cybercrime.....	28
7.7 Online Hate	29
7.8 Online Radicalisation and Extremism	29
8. Safer Use of Technology	30
8.1 Classroom Use	30
8.2 Managing Internet Access.....	31
8.3 Filtering and Monitoring	31
8.3.1 Decision Making	31

8.3.2 Decision Making	32
8.3.3 Monitoring	33
8.4 Managing Personal Data Online	33
8.5 Security and Management of Information Systems.....	34
8.5.1 Password Policy	35
8.6 Managing the Safety of our Website	35
8.7 Publishing Images and Videos Online.....	36
8.8 Managing Email.....	36
8.8.1 Staff Email.....	36
8.8.2 Learner Email	37
9. Social Media	37
9.1 Expectations	37
9.2 Staff Personal Use of Social Media	38
9.3 Pupils' Personal Use of Social Media	40
9.4 Official Use of Social Media	41
• Our official social media channels are:	41
10. Use of Personal Devices and Mobile Phones	43
10.1 Expectations.....	43
10.2 Staff Use of Personal Devices and Mobile Phones.....	44

10.3 Pupils' Use of Personal Devices and Mobile Phones	45
10.4 Visitors' Use of Personal Devices and Mobile Phones.....	47
10.5 Officially provided mobile phones and devices	47
11. Useful Links for Educational Settings.....	48
Pupil Acceptable Use of Technology Policy Agreements.....	50
Early Years -Year 2 - Acceptable Use Policy Agreement.....	51
The Agreement	51
Years 3-4 - Acceptable Use Policy Agreement.....	53
The Agreement	53
Years 5-8 - Acceptable Use Policy Agreement.....	56
The Agreement	56
Year 5-8 Acceptable Use Agreement Form	61
Template letter to Parents/carers for Early Years - Year 4 Children.....	62
Acceptable Use of Technology Template Statement and Forms for Parents/Carers	63
Meeting digital technology standards.....	Error! Bookmark not defined.
Filtering and monitoring standards	Error! Bookmark not defined.

1. Policy Aims

- This online safety policy has been adapted by Vinehall from 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 pupils 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 pupils 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 pupils, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, 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 but is linked to a member of the school. 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 non-criminal 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:
- Prevention of bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour Management policies
- Child protection and safeguarding policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security
- Image use policy

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 code of conduct also includes 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 Head 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, Ally Linney, 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 Katie Couldrey.
- 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 pupils 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, the Boarding Team, the Network Manager, mental health leads and Learning Support specialists) 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 pupils safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils 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, *as appropriate, to the safeguarding team, the senior management team and the 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 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 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 pupils (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 pupils

- 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 pupils 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.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating pupils 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 pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- We will support pupils 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 pupils 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.
 - Implementing appropriate peer education approaches.

- Providing online safety education and training as part of the transition programme across the key stages.
- 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 Pupils

- We recognise that some pupils 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 pupils.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the Head of Learning Support.

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 (alongside the safeguarding training) for all staff and governors on a regular basis, with at least annual updates.

- This will cover the potential risks posed to pupils (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 pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, 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, including offering specific online safety awareness training.
 - 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.

- 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 Head 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 pupils 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 Head will contact Sussex Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Pupils' 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 and safeguarding 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 Head, 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 safeguarding policy and within our prevention of 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.

- 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 safeguarding and prevention of bullying policies.
 - If content is contained on pupils electronic devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - Provide the necessary safeguards and support for all pupils 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 management 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 pupils 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 pupils 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 pupils, 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 pupils, 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.
- 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 pupils, 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, pupils 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 pupils 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 Head 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 Head 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 prevention of bullying policy.

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 pupils and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our safeguarding and child protection policy.
- If we are concerned that a member of staff or governor may be at risk of radicalisation online, the Head 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
 - Email
 - 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 pupils complies with copyright law and acknowledge the source of information.
- Supervision of pupils 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 pupils age and ability.
 - **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Pupils 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**
 - Pupils will be appropriately supervised when using technology, according to their ability and understanding.
- **Boarders**
 - We will balance children’s ability to take part in age-appropriate online use, 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, pupils 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 SMT 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 SMT 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, Network Manager 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 SMT 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 pupils; effective classroom management and regular education about safe and responsible use is essential.

8.3.2 Decision Making

- Education broadband connectivity is provided through (*Zen*).
- We use (*Smoothwall, Senso, Eset and Juniper*) which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. Our filtering provider is a member of the Internet Watch Foundation (IWF).
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- The filtering system blocks all sites on the Counter Terrorism Internet Referral Unit (CTIRU) list.
- We work with (*Smoothwall*) to ensure that our filtering policy is continually reviewed.

- If pupils discover unsuitable sites, they will be required to:
 - 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 Network Manager.
 - 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. This is achieved by:
 - *physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and active technology monitoring services.*
- If a concern is identified via monitoring approaches we will:
 - *Respond by alerting the DSL or deputies in line with the safeguarding and 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.

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, including:
 - 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 EYFS users.
 - All users are expected to log off or lock their screens/devices if systems are unattended.

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 3, all pupils are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords every six months.
 - 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 policies, 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 the Head or DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.

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, pupils and parents.

8.8.2 Learner Email

- Pupils will use provided email accounts for educational purposes.
- Pupils 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.

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 access to social media whilst using setting provided devices and systems on site.

- 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 prevention of bullying, allegations against staff, behaviour management and safeguarding & 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 pupils 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 pupils 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. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the Head.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Head.
- Any communication from pupils received on personal social media accounts will be reported to the DSL (or deputies).

9.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils 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 pupils under this age.
- Any concerns regarding pupils 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.
- Pupils 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

- Our official social media channels are:
 - *Facebook, Instagram and LinkedIn.*
- 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 Head.
 - 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 prevention of bullying, image/camera use, data protection, confidentiality and safeguarding & child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and pupils 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 pupils will be moderated possible.
- Parents and carers will be informed of any official social media use with pupils; 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 professional 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 and 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, pupils, parents and carers.
- Inform the DSL (or deputies) and/or the Head of any concerns, such as criticism, inappropriate content or contact from pupils.

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 Prevention of bullying, Behaviour Management, Safeguarding & 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 Early Years, 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, safeguarding & 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 Head, 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.
 - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) *and/or* Head.
- Staff will not use personal devices:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
 - Directly with pupils 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 Pupils' Use of Personal Devices and Mobile Phones

- Pupils 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 pupils' personal devices to be...
 - Kept by a member of staff and in a secure place outside of lesson times.
 - Use of 3G, 4G or 5G networks are not permitted in our setting, pupils must ensure that mobile data/data roaming is disabled.

- If a pupil needs to contact his/her parents or carers they will be allowed to use the school office phone.
- Parents of day children are advised to contact their child via the school office. Parents of boarders are aware of the times in which they can contact their children in the evenings or at weekends. Exceptions may be permitted on a case-by-case basis, as approved by the Head, for example to allow for time differences between countries.
- Personal devices will not be used by pupils during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- If members of staff have an educational reason to allow pupils 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.
- If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place.
- Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour management 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/searching-screening-and-confiscation)
- Pupils mobile phones or devices may be searched by a member of the leadership team or Houseparent, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers.

- If there is suspicion that material on a pupil'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.
- 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 Head of any breaches of 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 pupils/parents/carers is required.
- School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff
- School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

11. 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 \(eastsussex.gov.uk\)](http://Online Safety - Czone (eastsussex.gov.uk))

Pupil Acceptable Use of Technology Policy Agreements

We encourage teachers 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.

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.

Early Years -Year 2 - Acceptable Use Policy Agreement

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:

Years 3-4 - Acceptable Use Policy Agreement

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 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 accidentally 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 pre-arranged 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 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:

Years 5-8 - Acceptable Use Policy Agreement

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 on-line (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.
- 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 pre-arranged 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 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.

Year 5-8 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 - Year 4 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 or Head of Pre-Prep

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.
- 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: