Online Safety Policy and

Acceptable use of ICT agreement

Review cycle	1 / 2 / 3 years	**Date:** September 2026
Approved by	Full Governing Body / Executive Headteacher	
Changes made in this review cycle	September 2025 ● Updated using ESCC model policy 2025	
Linked policies	Health and Safety, Online Safety, Mental Health and Wellbeing, Supporting Pupils with Medical Conditions, preventing extremism and radicalisation.	
Signed	J. Procter	**Date:** September 2026
Position	Executive Headteacher	
Date of next Review	September 2027	

Contents

1. Policy Aims 8
2. Policy Scope 9
2.1 Links with other policies and practices 10
2.2 Online safety in community activities, after-school clubs and tuition 10
3. Monitoring and Review 11
4. Roles and Responsibilities 12
4.1 The leadership and management team and governors will: 12
4.2 The Designated Safeguarding Lead (DSL) will: 14
4.3 It is the responsibility of all members of staff to: 16
4.4 It is the responsibility of staff managing the technical environment to: 17
4.5. It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to: 17
4.6 It is the responsibility of parents and carers to: 18
5. Education and Engagement Approaches 18
5.1 Education and engagement with learners 18
5.2 Vulnerable Learners 20
5.3 Training and engagement with staff 21
5.4 Awareness and engagement with parents and carers 22
6. Responding to Online Safety Incidents and Concerns 22
6.1 Concerns about Learners' Welfare 23
6.2 Staff Misuse 24
7. Procedures for Responding to Specific Online Incidents or Concerns 24
7.1 Child-on-child online sexual violence and sexual harassment 24
7.2 Youth Produced Sexual Imagery ('Sharing nudes and semi nudes') 26
7.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation and County Lines) 28
7.4 Indecent Images of Children (IIOC) 29
7.5 Cyberbullying 31
7.6 Cybercrime 31
7.7 Online Hate 32
7.8 Online Radicalisation and Extremism 32

8. Safer Use of Technology 33
8.1 Classroom Use 33
8.2 Managing Internet Access 34
8.3 Filtering and Monitoring 34
8.3.1 Decision Making 35
8.3.2 Decision Making 36
8.3.3 Monitoring 37
8.4 Managing Personal Data Online 37
8.5 Security and Management of Information Systems 37
8.5.1 Password Policy (if not covered in other policies) 39
8.6 Managing the Safety of our Website 39
8.7 Publishing Images and Videos Online 40
8.8 Managing Email 40
8.8.1 Staff Email 41
8.8.2 Learner Email 41
8.9 Live Stream Lessons for Remote Learning 42
8.10 Management of Learning Platforms (*If used)* 44
8.11 Management of Applications (apps) used to Record Children's Progress (if used) 45
9. Social Media 46
9.1 Expectations 46
9.2 Staff Personal Use of Social Media 47
9.3 Learners' Personal Use of Social Media 50
9.4 Official Use of Social Media (Only include if setting has official social media)51
10. Use of Personal Devices and Mobile Phones 53
10.1 Expectations 53
10.2 Staff Use of Personal Devices and Mobile Phones 54
10.3 Learners' Use of Personal Devices and Mobile Phones 55
10.4 Visitors' Use of Personal Devices and Mobile Phones 57
10.5 Officially provided mobile phones and devices (*if provided)* 57
11. Useful Links for Educational Settings 57
12. Linking your Online Safety Policy with other school policies. 59
13. Disclaimer 61
Pupil Acceptable Use of Technology Policy Agreements (including Remote Learning if needed) 62
Early Year and Key Stage 1 (0-6) 63

The Agreement 63
Key Stage 2 (7-11) 65
The Agreement 65
Key Stage 3/4/5 (11-18) 68
The Agreement 68
Key Stage 3/4/5 Acceptable Use Agreement Form 73
Template letter to Parents/carers for Early Years – Key Stage 1 Children 74
Acceptable Use of Technology Template Statement and Forms for Parents/Carers 75
Staff, Visitor and Volunteers Acceptable Use of Technology (AUP) 78
Meeting digital technology standards in schools 92
Filtering and monitoring standards 92

1. Policy Aims

- This online safety policy has been adapted by Nutley Primary School involving staff, learners, governors and parents/carers, building on the East Sussex County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes account of the DfE statutory guidance Keeping Children Safe in Education, Early Years and Foundation Stage (*if applicable*) 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, and ever evolving but can be broadly categorised into four areas of risk:
    - **Content:** being exposed to illegal, inappropriate or harmful material.
    - **Contact:** being subjected to harmful online interaction with other users.
    - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
    - **Commerce/Contract:** risks such as online gambling, inappropriate advertising, phishing and or financial scams and sextortion (online sexual coercion and extortion of children).

2. Policy Scope

- We believe that online safety is an essential part of safeguarding and acknowledge its duty to ensure that all learners and staff are protected from potential harm online.
- We identify that the internet and associated devices, such as computers, tablets, mobile phones, smart watches and games consoles, are an important part of everyday life.
- We believe that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as "staff" in this policy) as well as learners, parents and carers. (*Amend staff roles as appropriate to the school*)
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.
- The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable to regulate the behaviour of students when they are off the school/academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. E.g. online bullying or online safety incidents which may take place outside of the school/academy but is linked to a member of the school/academy. The Behaviour in Schools guidance (2022) further reinforces this stating: *Maintained schools and academies' behaviour policies should set out what the school will do in response to 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:
- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- 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
- Mobile phone and social media policies (*if identified in separate documents*)

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

3. Monitoring and Review

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

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Hele Denton (Head of School) 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.
- 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:

- Understand that they have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- Be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Be responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to conduct their roles and train other colleagues, as relevant.
- Ensure that there is a system in place to allow for monitoring and support of those in school who conduct the internal online safety monitoring role.
- 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 collaborate 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 and making use of the government resource Plan technology for your school.
- Make use of the government guidance Generative AI: product safety expectations to ensure the safe use of generative artificial intelligence within the school.
- Ensure that online safety is embedded within a progressive preventative curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Recognise that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.
- Ensure that ALL members of staff receive regular, updated, and appropriate online safety training which is integrated, aligned and considered as part of the whole school safeguarding approach and know how to escalate concerns when identified.

- Support the DSL and any deputies by ensuring they have the additional time, funding, training, resources and support they need to conduct 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:

- Hold the lead responsibility for online safety, within their safeguarding role.
- 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.
- Collaborate with deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are conducted.
- Attend relevant governing body meetings/groups.
- Report regularly to Governors/headteacher/senior leadership team.
- 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.
- Be responsible for receiving reports of online safety incidents and managing them and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.

- Consult with staff (especially pastoral support staff, school nurses, IT technicians, senior mental health leads and SENCOs) on matters of safeguarding that include online and digital safety.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety, including filtering and monitoring and have the relevant knowledge and up to date training required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation.
- Keep up to date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Collaborate 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.

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 curriculum and policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Embed online safety education in curriculum delivery, wherever possible.
- Understand that online safety is a core part of safeguarding.

- 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.
- 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 regarding 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 learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities provided by Nutley Primary School.
- 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.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.

- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- We will establish and embed a broad, relevant and progressive online safety curriculum to raise awareness and promote safe and responsible online behaviour at school and at home amongst learners by:
    - Ensuring education regarding safe and responsible use precedes internet access.
    - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
    - Ensuring the curriculum builds on prior knowledge and is accessible for all pupils, including those with SEND or EAL.
    - Reinforcing online safety messages whenever technology or the internet is in use.
    - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation. This should include the use of generative AI tools and services.
    - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- We will support learners to read and understand the Acceptable Use Policies in a way which suits their age and ability by:
    - Acting as good role models in their use of digital technologies the internet and mobile devices.
    - Displaying age-appropriate acceptable use posters in all rooms with internet access.
    - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation. This should include information about whether school-owned devices are also monitored when not connected to the school network.
    - Rewarding positive use of technology.
    - Implementing appropriate peer education approaches.
    - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
    - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
    - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

Settings should include specific information in this section about how their community's needs have been identified and what action has been taken e.g. specific filtering requirements for children with EAL or SEND. This is especially important for special schools or settings with specialist units; policies should reflect the setting's circumstances.

- We recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs,

children with English as an additional language (EAL), EYFS (Early Years Foundation Stage) children and children experiencing trauma or loss.

- We recognise that children with cognitive difficulties may be unable to understand the difference between fact and fiction in online content and then may repeat the content/behaviours without understanding the consequences of doing so.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENCO Sian Leahy.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with ALL members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff and governors on a regular basis, with at least annual updates.
    - This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Ensure all new staff will receive online safety training as art of their induction programme.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.

- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
- Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.
- Providing them with information about our approach to filtering and monitoring as well as information about the types of things that children will be doing online.

6. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including breaches of filtering, youth produced sexual

imagery (sharing of nudes or semi-nudes/sexting), cyberbullying and illegal content.

- All members of the community will be directed to the DSL or headteacher in such circumstances.
- All reports will be taken seriously and will be dealt with as soon as is practically possible.
- All incidents should be logged.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- Safeguarding concerns and incidents, at level 3 or 4 on the Continuum of Need, should be reported to Single Point of Advice in line with East Sussex Safeguarding and Child Protection model policy.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Education Division Safeguarding Team.
- Where there is suspicion, that illegal activity has occurred contact the Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher/manager will contact Sussex Police first to ensure that potential investigations are not compromised.

6.1 Concerns about Learners' Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
    - The DSL (or deputies) will record these issues in line with our child protection policy.

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

6.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher/manager, 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.

- We recognise that sexual violence and sexual harassment between children can take place online and our staff will maintain an attitude of 'it could happen here.' Examples may include non-consensual sharing of nudes and semi-nudes images and videos, sharing of unwanted explicit content, upskirting, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.

  - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- We recognise that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum. See SRE and PSHE policies.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
  - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
  - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.

- If appropriate, make a referral to partner agencies, such as Children's Social Care and/or the Police.
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Sussex Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

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

- We recognise youth produced sexual imagery (known as "sharing nudes and semi nudes") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of sharing nudes and semi nudes (or sexting) by implementing preventative approaches, via a range of age and ability appropriate educational methods. (For example NSPCC Pantosaurus for younger learners).
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on/off site or using setting provided or personal equipment.

- We will not:

- View any images suspected of being youth produced sexual imagery, unless there is a clear need or reason to do so in order to safeguard the child or young person. If it is necessary to view the image(s) in order to safeguard the child or young person, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented- **in most cases, images or videos should not be viewed.** The UKCIS/DSIT guidance Sharing nudes and semi-nudes: advice for education settings working with children and young people provides information on the steps to be taken if an image does need to be viewed.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.

- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
  - Act in accordance with our child protection policy.
  - Ensure the DSL (or deputy) responds in line with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people, guidance.
  - Store the device securely.
    - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
  - Carry out a risk assessment which considers any vulnerability of learners involved, including conducting relevant checks with other agencies.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - Make a referral to Children's Social Care and/or the Police, as appropriate.
  - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support. This will include signposting to services such as *report remove* and *take it down.*
  - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.

- Consider the deletion of images in accordance with the UK Council for Internet Safety (UKCIS), Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance.
    - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

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

- We will ensure that all members of the community are aware of online child sexual abuse including exploitation and grooming, the consequences, approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. This can be accessed on the Nutley Primary School website.
- 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 and immediately inform the police via 101 (or 999 if a child is at immediate risk)
  - Conduct a risk assessment which considers any vulnerabilities of pupil(s) involved (including conducting relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
  - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/.

- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.

- If learners at other settings are believed to have been targeted, the DSL (or deputy) will contact the Police.

7.4 Indecent Images of Children (IIOC)

- We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet service provider (ISP) which implements appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Police.
- If made aware of IIOC, we will:
    - Act in accordance with our child protection policy.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
    - Ensure that the DSL (or deputy DSL) is informed, who will investigate the incident.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
    - Ensure that the DSL (or deputy DSL) and headteacher are informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
    - Ensure that any copies that exist of the image, for example in emails, are deleted once directed to by the police.
    - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social services (as appropriate).
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
    - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the headteacher/manager 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 anti-bullying policy on the Nutley Primary School website.

7.6 Cybercrime

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

7.7 Online Hate

- Online hate content, directed towards or posted by specific members of the community will not be tolerated at our setting and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.

- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex Police.

7.8 Online Radicalisation and Extremism

- We will ensure that all members of the community are made aware of the role of the internet as a tool for radicalisation.
- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site. Smoothwall is in place to block extremist material.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that a member of staff or governor may be at risk of radicalisation online, the headteacher/manager will be informed immediately, and action will be taken in line with the child protection and allegations policies.

8. Safer Use of Technology

8.1 Classroom Use

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

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

- All devices will be used in accordance with our Acceptable Use Policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
    - *Settings should list search tools suggested for staff and pupils to use. Examples could include SWGfL Swiggle, Dorling Kindersley find out and Google Safe Search.*
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
    - **Early Years Foundation Stage and Key Stage 1**
        - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners age and ability.
    - **Key Stage 2**
        - Learners will use age-appropriate search engines and online tools.

- Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

8.2 Managing Internet Access

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

8.3 Filtering and Monitoring

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

8.3.1 Decision Making

- Our governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking," as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances and is reviewed at least annually by the DSL, IT service provider and the governor responsible for safeguarding/online safety. A review will also be conducted 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 conducting the review.

- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate using the Safer Internet Centre guidance on appropriate filtering and appropriate monitoring.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

8.3.2 Decision Making

- Education broadband connectivity is provided through South East Grid.

- We use Smoothwall which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- 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 South East Grid/ Smoothwall to ensure that our filtering policy is continually reviewed.
- If learners 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 technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Sussex Police or CEOP.

8.3.3 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices and personal devices which connect to the school infrastructure/network This is achieved by:
    - *Physical monitoring (supervision), monitoring internet and web access (reviewing logfile information) and/or active/pro-active technology monitoring services.*
- If a concern is identified via monitoring approaches we will:
    - *DSL or deputies will respond in line with the child protection policy.*
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

8.4 Managing Personal Data Online

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

8.5 Security and Management of Information Systems

- We adhere to and meet the DfE cybersecurity standards.

- We take appropriate steps to ensure the security of our information systems, 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 youngest users*. (Note: this should be in place for all except Early Years Foundation Stage children, possibly year one children and some learners with SEND).
    - All users are expected to log off or lock their screens/devices if systems are unattended.
    - Further information about technical environment safety and security can be found at: Data Protection and Information Security policy. https://www.nutleyprimaryschool.org.uk/policies-procedures

8.5.1 Password Policy (if not covered in other policies)

- 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 learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
    - Use strong passwords for access into our system.
    - Use a separate password for your work and personal accounts.
    - Change their passwords annually.
    - 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.
    - If you use a deny list for automatic blocking of common passwords, use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. The National Cyber Security Centre recommends using passwords made up of 3 random words. Enforce account lockouts after a number of failed attempts and require service provider or network manager permission to unlock.
    - Store passwords securely.

8.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright.

- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

8.7 Publishing Images and Videos Online

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

8.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
    - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately inform Helen Denton, Head of School, if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

8.8.1 Staff Email

- The use of personal email addresses by staff for any official setting business is not permitted.
    - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

8.8.2 Learner Email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

8.9 Live Stream Lessons for Remote Learning

- Live stream is a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

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

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

- Two members of staff will be 'within the room' when conducting a live stream session with pupils. If the session is being run from school and both adults are there, then they can be physically within the same room. If one or both adults are working remotely then this means that two adults will need to be present within the video call, and they should both be there before the pupils dial in.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or recording features if these cannot be disabled.
- It is the responsibility of the staff member to act as a moderator, raising any issues of suitability (dress, setting, behaviour etc.) with the child and/or parent immediately and ending the online interaction if necessary.
- Sessions will be planned and scheduled for during school hours.
- Parents will be contacted to advise that the session is taking place and they and the child should consent to abide to an acceptable use agreement covering issues such as not recording the session, not using the live chat feature, being appropriately dressed etc.

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

Live Stream from other providers

- When directing learners to any content from other providers, its suitability and appropriateness will be checked.
- Where that content may be live streamed, the safeguarding aspect of how that content is being delivered will be considered e.g. how children are able to interact, how is content and interactions being monitored/moderated etc?
- For one off live stream events, a member of staff will monitor the content along with the interactions/behaviour of the learners taking part.
- When/if multiple sessions are being run at various times during the school day, school leaders will check that they are satisfied with the safeguarding policy of the provider(s) and then, monitor some sessions to check they are in accordance with the policy.
- We are aware that our filtering and monitoring systems may not necessarily prevent inappropriate content from being shared in a live-streamed event as this is happening in real-time.

Using video calls for 1:1 sessions with children

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

8.10 Management of Learning Platforms (*If used)*

- We use GSuite Google Classroom as our official learning platform.
- Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.

- Any concerns about content on the LP will be recorded and dealt with in the following ways:

  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the site administrator will remove the material.
  - Access to the LP for the user may be suspended.
  - The user will need to discuss the issues with a member of leadership before reinstatement.
  - A learner's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited onto the LP by a member of the leadership; in this instance, there may be an agreed focus or a limited time slot.

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

- We use ARBOR to track learners progress and share appropriate information with parents and carers.
- The Head of School is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
  - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

9. Social Media

9.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of our community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of our community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of our community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others or that could damage the reputation of the school or individual within it.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
  - The use of social media during setting hours for personal use is not permitted.
  - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of our community on social media, should be reported to the DSL (or deputy) and will be managed in

accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct/ Staff behaviour policy as part of Acceptable Use Policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
    - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.
    - Opting out of public listings on social networking sites.
    - Logging out of accounts after use.
    - Keeping passwords safe and confidential and using two factor authentication wherever possible.
    - Ensuring staff do not represent their personal views as that of the setting.

- Members of staff are encouraged not to identify themselves as employees of our setting on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners, parents, and carers

- Communication with children both in the offline world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web cams and other hand-held devices. (Given the ever-changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour.'
- Staff should not give out any personal contact details.
- On school trips, staff should have a school mobile phone rather than having to rely on their own device.
- Staff should not accept friend requests from pupils, past or present. If a member of staff feels that this is necessary, they should first seek guidance from the DSL

or a senior leader. If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools. Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputies) and/or the headteacher/manager. (See *Staff Behaviour Policy/ Code of Conduct for further information*)

- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the headteacher/manager.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

9.3 Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying, behaviour and Acceptable Use Policies.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools and the sharing of inappropriate images or messages that may be considered threatening, hurtful or defamatory to others.
- Learners will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords and two factor authentication where possible.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.
- To remove a social media conversation thread if they are the administrator of such a thread that may have been used in an inappropriate way such as with threatening, hurtful or defamatory content.

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

- Our official social media channels are:
  - *List details e.g. Twitter link; Facebook page link; YouTube channel link.*
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher/manager.
  - 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 and, where possible, run *and/or* linked *to/from* our website.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.

- Official social media use will be conducted in line with existing policies, including anti-bullying, image/camera use, data protection, confidentiality and child protection.
    - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
    - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
    - Any official social media activity involving learners will be moderated possible.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
    - Sign our social media acceptable use policy.
    - Always be professional and aware they are an ambassador for the setting.
    - Disclose their official role *and/or* position but make it clear that they do not necessarily speak on behalf of the setting.
    - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.

- Always act within the legal frameworks they would adhere to within the workplace including libel, defamation, confidentiality, copyright, data protection and equalities laws.
- Ensure that they have appropriate consent from both pupils and parents before sharing images on the official social media channel.
- Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
- Not engage with any direct or private messaging with current, or past, learners, parents and carers.
- Inform their line manager, the DSL (or deputies) and/or the headteacher/manager of any concerns, such as criticism, inappropriate content or contact from learners.

10. Use of Personal Devices and Mobile Phones

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

10.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Anti-bullying, Behaviour, Child Protection and Staff Code of Conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.

  - All members of our community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of our community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as toilets or any areas where pupils may be changing e.g for PE.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.

- All members of our community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

10.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place such as the staff room, in a fastened bag or in a locked cupboard 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.

  - Not use personal devices during teaching periods, unless written permission has been given by the headteacher/manager, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting pupils or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies).
- Staff will not use personal devices:
  - To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - Directly with learners and will only use work-provided equipment during lessons or educational activities.

- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy.
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

10.3 Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- We expect learners' personal devices and mobile phones to be:
- Pre-arranged to be securely stored in a locked cupboard in the school office during school hours.
- Use of 3G, 4G or 5G networks are not permitted in our setting, learners must ensure that mobile data/data roaming is disabled.

- If a learner needs to contact his/her parents or carers they will be allowed to use a setting phone.
- Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the headteacher.
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices (including smart watches) must not be taken into examinations.
- Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
- Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be conducted in accordance with our Behaviour policy. *See* www.gov.uk/government/publications/searching-screening-and-confiscation)
- A member of the leadership team may search learners mobile phones or devices, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation)
- Mobile phones and devices that have been confiscated will be released to parents or carers (list details e.g. at the end of the day, week, term etc.)
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

10.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including Governors, volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or headteacher/manager of any breaches our policy.

10.5 Officially provided mobile phones and devices (*if provided)*

- Members of staff will be issued with a work phone number and email address, where contact with learners/parents/carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed of used by members of staff.
- Setting 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
- Education Safeguarding Team : education.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
- 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
- 360 Safe Self-Review tool for Early Years: Online Safety Self-Review Tool | 360 Early Years | 360 Early Years
- London Grid for Learning Online Safety Audit tool for schools. OS Audit - Online Safety Audit from LGfL | LGFL
- Get Safe Online: www.getsafeonline.org
- Action Fraud : www.actionfraud.police.uk

- An online safety toolkit is available. Please email education.safeguarding@eastsussex.gov.uk

National Links and Resources for Professionals/Parents/Carers

There is a wealth of information available to support schools and parents/carers to keep children safe online.
See Keeping Children Safe in Education 2024- Pg.164 for more resources.

12. Linking your Online Safety Policy with other school policies

This online safety policy provides educational settings with a framework to develop their online safety ethos and enables leaders and managers to detail strategic approaches and considerations, with regards to the safer use of technology. The policy should be used as part of an effective whole school approach to online safety. All staff in schools need to understand their responsibilities to ensure that children and young people can use the internet appropriately and safely. Schools should ensure online safety is a running and interrelated theme whilst implementing this policy.

The online safety policy should be recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the

Designated Safeguarding Lead (DSL).

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

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

2.0	References the Education and Inspections Act 2006 relating to behaviour outside of school
4.3 4.6	References Acceptable Use Policies
4.5	References behaviour outside of school
6	References safe and appropriate behaviour online and the importance of not posting any content, comments, images, or videos which could cause harm, distress, or offence to members of the community
7.1 and 7.5	References the school's anti-bullying policy
7.7	References how online hate will be responded to in line with existing policies, including anti-bullying and behaviour.
9.1	References behaviour on social media platforms
9.3	References to social media threads and administrators of threads
10.1	References personal mobile devices and possible content that might be offensive, derogatory or would otherwise contravene our behaviour or child protection policies
10.3	References expectations for learner's mobile phone use

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

This policy template requires leaders, managers, and DSLs to adapt the content to

include specific local information such as their own named points of contact, as well as their specific procedures and expectations. These decisions and details will vary from school to school, so this template should be used as a starting framework.

13. Disclaimer

The original template for this model policy was created by the Education People on behalf of East Sussex County Council in 2016. Copyright of these materials is held by The Education People; this must be acknowledged when the template is used.

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

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

Early Years and Key Stage 1 (0-6)

The Agreement

This agreement is intended to help our younger pupils understand:

- How to stay safe while using the internet and other digital technologies for educational, personal, and recreational use.
- That they must use school systems in a responsible way, to ensure that there is no risk to their own safety or to the safety and security of the systems and other users.
- I understand that the Nutley Primary School Acceptable Use Policy will help keep me safe and happy online.

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 only click on online links and buttons when I know what they do. If I am not sure, I ask an adult first.
- I will only use activities that an adult has told or allowed me to use.
- I keep my personal information and passwords safe.
- I will be kind to others online when I am sending messages.
- I know Nutley Primary School can see what I am doing online when I use Nutley Primary School computers/tablets and name of any specific Nutley Primary School services and systems learners are expected to use, including if I use them at home. 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 do not 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.

Child's Name:

Class:

Date:

Parent's Name:

Parent's Signature:

Date:

Key Stage 2 (7-11)

The Agreement

This Acceptable Use Policy Agreement is intended to ensure:

- that pupils at Nutley Primary School will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- I understand that the Nutley Primary School Acceptable Use Policy will help keep me safe and happy online at home and at Nutley Primary School.

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 Nutley Primary School 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.
- 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 Nutley Primary School,
- I know that all Nutley Primary School devices/computers and systems are filtered and monitored.

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

- I will be polite and sensible when I message people online.
- I will not be rude or hurt someone's feelings online.
- I will not purposely exclude others from online activities.
- I will not look for bad language, inappropriate images or violent or unsuitable games or content, and if I accidently come across any of these, I will report it to a teacher or adult in Nutley Primary School 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 of any of the teaching resources made available except for my own personal use.
- I will not take, use, share, publish or distribute images of others without their permission.
- I will not share any access links to these remote learning sessions with others.
- I understand that I must behave online as I would in a classroom.
- I will only use the chat feature for work related discussions.
- I have read and talked about these rules with my parents/carers.
- I understand that if I do not follow this agreement, I may not be allowed to use the internet at Nutley Primary School.

Child's Name:

Child's Signature:

Class:

Date:

Parent's Name:

Parent's Signature:

Date:

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

This letter can be amended to use with older children.

Dear Parents and Guardians,

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

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

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

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

Signed by DSL/Head etc.

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

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

- I have read – and discussed with my child the pupil Acceptable Use of Technology Agreement Policy (AUP) for Nutley Primary School and understand that this AUP will help keep my child safe online.
- I understand that the AUP applies to my child's use of Nutley Primary School 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 Nutley Primary School devices and systems may be monitored for safety and security reason to keep my child safe. This monitoring will take place in accordance with data protection, privacy, and human rights legislation and further information about the school's approach can be found *(Insert link to where this information can be found)*
- 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;
- 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 Nutley Primary School 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 Nutley Primary School will take every reasonable precaution, including implementing appropriate monitoring and filtering systems, to ensure my child is safe when they use Nutley Primary School devices and systems. I understand that Nutley Primary School 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 learning to be used on Nutley Primary School 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 Nutley Primary School community.
- I understand that Nutley Primary School 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 Nutley Primary School or other relevant organisations if I have concerns over my child's or other members of the Nutley Primary School 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 Nutley Primary School
- I will support the Nutley Primary School 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.

Child's Name:

Class:

Date:

Parent's Name:

Parent's Signature:

Date:

Staff, Governors, Visitors and Volunteers Acceptable Use of Technology Policy (AUP)

Acceptable Use of Technology for Staff, Visitors and Volunteers Sample Statements

Staff (AUP)

As a professional organisation with responsibility for safeguarding, all members of staff, Governors, visitors and volunteers are expected to use Nutley Primary School IT systems in a professional, lawful, and ethical manner. To ensure that members of the school community understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for pupils they are asked to read and sign the staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of the school community teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all members of the school community understand Nutley Primary School expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that Nutley Primary School systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this Acceptable Use of Technology Policy (AUP) applies to my use of technology systems and services, either provided to me by Nutley Primary School or accessed by me as part of my role within Nutley Primary School, professionally and personally, both on and offsite. This may include my use of devices such as laptops, mobile phones, tablets, digital cameras, as well as IT systems and networks, email. data and data storage, remote learning systems and communication technologies.
2. I understand that Nutley Primary School Acceptable Use of Technology Policy (AUP) should be read and followed in line with the Nutley Primary School child protection/online safety policy and the staff behaviour policy/code of conduct
3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the Nutley Primary School ethos, Nutley Primary School staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of Nutley Primary School **devices and systems**

4. I will only use the equipment and internet services provided to me by Nutley Primary School for example Nutley Primary School provided laptops, tablets, mobile phones and internet access, when working with pupils.
5. I understand that any equipment and internet services provided by Nutley Primary School are intended for education purposes and/or professional use and should only be accessed by members of staff and Governors, or visitors or volunteers with support from a member of staff. Reasonable personal use of setting IT systems and/or devices by staff, Governors, visitors and volunteers is allowed; this use at the <School/Setting>'s discretion and can be revoked at any time.
6. Where I deliver or support remote/online learning, I will comply with the Nutley Primary School remote/online learning AUP.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

8. I will use a 'strong' password to access Nutley Primary School systems. **Use a password with at least 8 characters. If you do not use a deny list, use a password with at least 12 characters or a biometric test. The National Cyber Security Centre recommends using passwords made up of 3 random words.**
9. I will protect the devices in my care from unapproved access or theft. **Detail how this should be achieved, for example not leaving devices visible or unsupervised in public places.**
10. I will respect Nutley Primary School system security and will not disclose my password or security information to others.
11. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager. **Amend as appropriate.**
12. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.
13. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including
    - All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary, and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online, or accessed remotely.
    - Any data being removed from the Nutley Primary School site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by Nutley Primary School.

14. I will not keep documents which contain Nutley Primary School related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the Nutley Primary School learning platform to upload any work documents and files in a password protected environment.

15. I will not store any personal information on the Nutley Primary School IT system, including Nutley Primary School laptops or similar device issued to members of staff, which is unrelated to Nutley Primary School activities, such as personal photographs, files or financial information.
16. I will ensure that Nutley Primary School owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
17. I will not attempt to bypass any filtering and/or security systems put in place by Nutley Primary School.
18. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT Support Provider.
19. If I have lost any Nutley Primary School related documents or files, I will report this to the ICT Support Provider/Team/lead (named contact) and Pioneer Federation Data Protection Officer (Roger Simmons) as soon as possible.
20. Any images or videos of pupils will only be used as stated in the Nutley Primary School camera and image use policy. I understand images of pupils must always be appropriate and should only be taken with Nutley Primary School. provided equipment and only be taken/published where pupils and/or parent/carers have given explicit written consent.

Classroom practice

21. ***If a staff member** - I understand that it is part of my roles and responsibilities to ensure that appropriate filtering and monitoring is implemented by Nutley Primary School. as detailed in the child protection and online safety policies, and as discussed with me as part of my induction and/or ongoing safeguarding and child protection staff training. **Leaders should ensure the online safety or child protection policy includes specific details for staff relating to regarding expectations, applicable roles and responsibilities for appropriate filtering and monitoring.**

22. If there is failure in the filtering software or abuse of the filtering or monitoring systems, for example, I witness or suspect accidental or deliberate access to illegal, inappropriate or harmful material, I will report this to the DSL, in line with the Nutley Primary School child protection/online safety policy. **Leaders should ensure this is detailed in the child protection or online safety policy. If this is not addressed in a separate policy, additional detail should be incorporated in this AUP.**
23. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed in the child protection, and online safety policies.
24. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:
    - exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.
    - creating a safe environment where pupils feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
    - involving the Designated Safeguarding Lead (DSL) Helen Denton or a deputy Amy Marhsall/ Sarah Debenham as part of planning online safety lessons or activities to ensure support is in place for any pupils who may be impacted by the content.
    - informing the DSL and/or leadership team if I am teaching topics which could create unusual activity on the filtering logs, or if I believe the filtering system is placing unreasonable restrictions on teaching, learning or administration.
    - make informed decisions to ensure any online safety resources used with pupils is appropriate.
25. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

26. I have read and understood the Nutley Primary School. mobile and smart technology and social media policies which addresses use by pupils and staff, Governors, visitors and volunteers.
27. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff behaviour policy/code of conduct and the Nutley Primary School mobile technology policy and the law.

Online communication, including use of social media

28. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policy, staff behaviour policy/code of conduct, social media policy and the law.
29. As outlined in the staff behaviour policy/code of conduct and Nutley Primary School. social media policy:
    - I will take appropriate steps to protect myself and my reputation, and the reputation of Nutley Primary School. online when using communication technology, including the use of social media.
    - I will not discuss or share data or information relating to pupils staff, Nutley Primary School business or parents/carers on social media

30. My electronic communications with current and past pupils and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.
    - I will ensure that all electronic communications take place in a professional manner via Nutley Primary School. approved and/or provided communication channels and systems, such as a Nutley Primary School. email address, user account or telephone number.
    - I will not share any personal contact information or details with pupils such as my personal email address or phone number.
    - I will not add or accept friend requests or communications on personal social media with current or past pupils and/or their parents/carers.
    - If I am approached online by a current or past pupils or parents/carers, I will not respond and will report the communication to my line manager and (Helen Denton) Designated Safeguarding Lead (DSL).
    - Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL.

Policy concerns

31. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.
32. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.
33. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of Nutley Primary School. into disrepute.
34. I will report and record any concerns about the welfare, safety or behaviour of pupils or parents/carers online to the DSL in line with the Nutley Primary School. child protection policy.
35. I will report concerns about the welfare, safety, or behaviour of staff online to the Head of School, in line with Nutley Primary School child protection policy and/or the allegations against staff policy.

Policy Compliance and Breaches

36. If I have any queries or questions regarding safe and professional practise online, either in Nutley Primary School. or off site, I will raise them with the DSL.
37. I understand that the Nutley Primary School. may exercise its right to monitor the use of its devices information systems to monitor policy compliance and to ensure the safety of pupils and staff. This includes monitoring all Nutley Primary School. provided devices and Nutley Primary School. systems and networks including Nutley Primary School. provided internet access, whether used on or offsite and may include the interception of messages and emails sent or received via Nutley Primary School. provided devices, systems and/or networks. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.
38. I understand that if Nutley Primary School. believe that unauthorised and/or inappropriate use of Nutley Primary School. devices, systems or networks is taking place, Nutley Primary School. may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
39. I understand that if Nutley Primary School believe that unprofessional or inappropriate online activity, including behaviour which could bring Nutley Primary School into disrepute, is taking place online, Nutley Primary School may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.
40. I understand that if Nutley Primary School suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Nutley Primary School Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Date:…….

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

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

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

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

- I will be aware of and understand my responsibilities when delivering remote lessons.
- I understand that communication with children both off and online must take place within explicit professional boundaries.
- I will be aware of the following policies and procedures:
    - Safeguarding and Child Protection Policy
    - Online Policy and Staff Acceptable Use Policy
    - Behaviour policy
    - Staff Code of Conduct
    - Social Media Policy

- I will not use any personal accounts to communicate with pupils and/or parents/carers.
- I will not seek to communicate/make contact or respond to contact with pupils outside of the purposes of my work or outside of school hours.
- I will use work provided equipment where possible e.g., a Nutley Primary School laptop, tablet, or other mobile device – where not possible clear expectations in need to be place in relation to safeguarding and data security when using personal devices e.g., using strong passwords, suitable levels of encryption, logging off when not in use etc.
- I am aware that online bullying is a safeguarding issue and that any incidents of this must be reported to the DSL as per Nutley Primary School. Safeguarding procedures.
- I will report any suspected misuse or problem to the Online Safety Coordinator (DSL) or Network Manager for investigation / action / sanction.
- If I am a class teacher, I will ensure all my pupils have understood and returned the Pupil Remote Learning Home Agreement.
- If I am a class teacher, I will provide remote pastoral care for my class.
- I will continue to look out for signs that a child may be at risk whilst teaching remotely.
- I understand that it is best practice that staff will guide pupils to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches., e.g. Google Images.
- I will be mindful of the added pressure that remote learning can add to any household and, in particular, in a household with more vulnerable children,
- If I am a SEN or EAL teacher, I will provide assistance to teachers who require help to differentiate and will ensure contact with pupils and their parents who are likely to require further assistance.
- If I am a Form /Class teacher, I will ensure I have regular contact with my class.
- I will make contact with pupils only via Nutley Primary School provided email accounts or logins.
- When recording videos and for live lessons I understand that I must wear appropriate clothing.

- I understand that for live lessons at least two members of staff should be present and where this is not possible the leadership team approval will be sought.
- I understand that live lessons should be recorded and backed up on Teams Streams/school server, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.
- I understand that any 1-1 live lessons need to be pre-arranged, with written parental consent given and that two adults need to be present. Where 1-1 sessions may be necessary these sessions must be recorded and saved to the school server where this can be reviewed at any time.
- I will not record lessons or meetings using personal equipment.
- I understand that any computers used for such recordings or live lessons should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral/blurred background.
- I understand that live lessons should be recorded and backed up on Teams Streams/school server, so that if any issues were to arise, the video can be reviewed and I understand that these recordings will be kept in accordance with data protection.
- I understand that all my language must be professional and appropriate, including if any of my family members are in the background.
- I will not give out my personal details.
- I will not take images of pupils for my own personal use.
- I will not display or distribute images of pupils unless they have parental consent to do so (and, where appropriate, consent from the child)
- At the beginning of each session I will remind pupils of behaviour expectations and reporting mechanisms at the start of the session, including the use of microphones and chat features.
- I will remind pupils to report concerns during remote and/or live streamed sessions:
- If inappropriate language or behaviour takes place, pupils involved will be removed by staff, and concerns will be reported to name/role.

- Inappropriate online behaviour will be responded to in line with existing policies such as acceptable use of technology, allegations against staff, anti-bullying, and behaviour.
- I will report any safeguarding concerns will be reported to Nutley Primary School. Designated Safeguarding Lead, in line with our child protection policy.

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

Name:

Date:

Meeting digital technology standards in schools

Filtering and monitoring standards

Task/responsibility	Notes
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	
Responsibility: Gov	

Task: Identify and assign a member of the SLT to be responsible for ensuring that the standards are met	
Responsibility: Gov **Task**: Identify and assign a governor to be responsible for ensuring that the standards are met	
Responsibility: Gov **Task**: Identify and assign the roles and responsibilities of staff and third parties (incl. external service providers)	
Responsibility: Gov **Task**: Is it possible to make "prompt" changes to provision?	
Responsibility: SLT with support from DSL and ITSP **Task**: Procuring filtering and monitoring systems	
Responsibility: SLT **Task**: Document decisions about what is blocked or allowed and why	
Responsibility: SLT **Task**: Review the effectiveness of your provision (and provide evidence)	
Responsibility: SLT **Task**: Oversee reports	
Responsibility: SLT **Task**: All staff have received appropriate and up to date training and understand their role	
Responsibility: SLT **Task**: All staff follow policies and procedures and processes around online safety and filtering and monitoring	
Responsibility: SLT **Task**: All staff act on reports and concerns	
Responsibility: DSL **Task**: Oversee and act on filtering and monitoring reports	
Responsibility: DSL	

Task: Oversee and act on safeguarding concerns	
Responsibility: DSL **Task**: Oversee and act on checks to monitoring systems	
Responsibility: ITSP **Task**: Maintain filtering and monitoring systems	
Responsibility: ITSP **Task**: Provide filtering and monitoring reports	
Responsibility: ITSP **Task**: Complete actions following concerns or checks to systems	

Task/responsibility	**Notes**
You should review your filtering and monitoring provision at least annually	
Responsibility: Joint **Task**: Carry out reviews of the filtering and monitoring provision at least annually	
Responsibility: Joint **Task**: Carry out checks which are informed by the review to ensure systems are working	
Responsibility: Joint **Task**: Understand the risk profile of pupils – incl. those in vulnerable groups, age, SEND, EAL	
Responsibility: Joint **Task**: What does the filtering system block/allow and why?	
Responsibility: Joint **Task**: Are there any outside safeguarding influences that should be considered (e.g., county lines)	Ensure that this is relevant to your school or setting
Responsibility: Joint	

Task: Are there any relevant safeguarding reports that could/should impact on filtering and monitoring?	
Responsibility: Joint **Task**: How digitally resilient are pupils?	
Responsibility: Joint **Task**: What does the RHSE and PSHE curricula cover and how might this impact on filtering?	
Responsibility: Joint **Task**: How are devices used within school? (e.g., BYOD)	
Responsibility: Joint **Task**: What related safeguarding and technology policies are in place?	
Responsibility: Joint **Task**: What checks are in place – how are resulting actions handled? *Checks should be undertaken from a safeguarding **and** an IT perspective*	
Responsibility: Joint **Task**: How often are checks carried out, what is checked? *Filtering should be tested – log what is done and the results that are obtained – make changes as a result. Different devices should be used when conducting checks to get a good overview of what is or is not accessible.*	
Responsibility: Joint **Task**: How does monitoring work? *How often are reports received – are these in real time – what thresholds are in place – are these fit for purpose?*	
Responsibility: Joint **Task**: Does filtering and monitoring work on new	

devices? Is this checked before they are given to staff/pupils?	
Responsibility: Joint **Task**: Review blocklists and modify in line with any changes to safeguarding risks	
Responsibility: Joint **Task**: Check your system using the SWGfL testing tool to see that it is blocking access to illegal child sexual abuse material, unlawful terrorist content, adult content	

Task/responsibility	**Notes**
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	
Responsibility: DSL and ITSP **Task**: Is your filtering provider a member of the IWF?	
Responsibility: DSL and ITSP **Task**: Does your filtering provider use the IWF list?	
Responsibility: DSL and ITSP **Task**: Does your filtering provider use the CTIRU list?	
Responsibility: DSL and ITSP **Task**: Are you blocking access to adult content?	
Responsibility: DSL and ITSP **Task**: Is filtering applied to all accounts including guest accounts? (Staff, pupils)	
Responsibility: DSL and ITSP **Task**: Is filtering applied to all school owned devices?	
Responsibility: DSL and ITSP **Task**: Is filtering applied to any device which connects to the school broadband connection?	
Responsibility: DSL and ITSP **Task**: Do you filter all internet feeds including any backup connection?	

Responsibility: DSL and ITSP **Task**: Is filtering differentiated by age and ability of pupils?	
Responsibility: DSL and ITSP **Task**: Can filtering handle multilingual content, images, misspellings, abbreviations?	
Responsibility: DSL and ITSP **Task**: Can filtering identify VPNs and proxy services and then block them?	
Responsibility: DSL and ITSP **Task**: Can filtering system provide alerts when access to content has been blocked?	
Responsibility: DSL and ITSP **Task**: Does filtering work on mobile devices? *Is there evidence, have you checked?*	
Responsibility: DSL and ITSP **Task**: Does filtering work on app content? *Is there evidence, have you checked?*	
Responsibility: DSL and ITSP **Task**: Will the filtering system identify the IP address, device name and ID and where possible the individual who has attempted to access unsuitable or illegal content?	

Task/responsibility	**Notes**
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	
Responsibility: ITSP **Task**: Are monitoring systems working as expected?	
Responsibility: ITSP **Task**: Are reports on pupil device activity available?	
Responsibility: ITSP	

Task: Are IT staff given safeguarding training including online safety training?	
Responsibility: ITSP **Task**: Are IT staff reporting any issues (safeguarding concerns to the DSL)?	
Responsibility: All staff **Task:** Are the wider staff body reporting safeguarding concerns to the DSL	
Responsibility: All staff **Task:** Are the wider staff body providing effective supervision of pupils?	
Responsibility: All staff **Task:** Are the wider staff body taking steps to maintain awareness of how devices are being used by pupils?	

Key:

Gov - Governor with designated responsibility for online safety/safeguarding

DSL - Designated safeguarding lead

SLT - Member of the senior leadership/senior management team

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

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

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