# NAS Online Safety Policy - SO-0106

| | |
|---|---|
| Date of Issue | October 2020 |
| Date reviewed | September 2023 |
| Date of next review | September 2024 |
| Version Number | 3.2 |
| Policy Lead | Brendan Walsh |
| Distribution | Education Directorate |
| Date ratified by board | TBC |
| Responsible governor | TBC |

**The Designated Safeguarding Lead for the school is Sara White**

**Overview**

Pupils at the school have the right to access new and emerging technologies as part of their education and care. These technologies are a vital part of the lives of many people with autism and the school is committed to promoting pupils' development of the skills, knowledge and understanding to communicate, create, investigate, play and relax online. The school provides technology for pupils as well as providing a network.

The school recognises that online activity brings with it potential risks, which fall into the main categories below:

Content:

Age-inappropriate content that a child may come across online could be:

- commercial – such as adverts, spam or sponsorship
- aggressive – such as violent and hateful content
- sexual – inappropriate or unwelcome sexual content
- content that promotes negative values – for example biased, racist or misleading information.

Contact:

If a child is actively engaged in the online world, they may become involved in interactions that could be harmful to them. This could be:

- commercial – such as tracking the sites a child has looked at or harvesting their personal information
- aggressive – for example being bullied, harassed or stalked
- sexual – receiving sexualised requests from others, harassment or being groomed
- contacts who promote negative values – for example making 'friends' who persuade a child to carry out harmful activities.

Conduct:

Without meaning to, a child may behave in a way that puts them and/or others at risk. For example, they may become involved in:

- inappropriate commercial activity - illegal downloading, hacking, using the dark web or getting involved in financial scams

- aggressive behaviour – bullying or harassing someone else
- sexualised behaviour – creating or uploading indecent images, sexually harassing others
- creating content that promotes negative values – providing misleading information to others

Commerce:

- risks such as online gambling
- phishing or financial scams (which can be serious risk for some autistic people)
- inappropriate advertising

Our primary aim with regard to online safety is to give pupils the ability to stay safe online – both inside the school and beyond. We aim to do this through education, embedding online safety in every aspect of the curriculum and working with parents/carers, siblings and others to promote safe use of technology. This online safety policy (and the associated procedures) lay out the ways in which we keep pupils safe while providing this education.

As a school we have specific, statutory responsibilities to ensure and promote the safety and well-being of our pupils and this applies to the online environment. A number of laws and statutory government guidance applies in this area, see appendix 2 for a full list of legislation and guidance. Online safety is an integrated part of the school's statutory safeguarding responsibilities.

**Aims**

The school aims to provide pupils with the skills, knowledge and understanding to keep themselves safe online within the school and beyond, now and in the future. This policy gives guidance on providing a safe environment in which pupils may develop their own online safety skills.

**Roles & Responsibilities**

**Managing Director of Education and Children's Services and the NAS SGG (Schools Governance Group)**

Responsible for the approval of the Online Safety Policy, for reviewing the effectiveness of the policy and for overseeing revisions of the policy. They will also act as a 'friendly critic' and ensure:

- regular meetings with the school Online Safety Coordinator
- regular monitoring of online safety incident logs
- regular monitoring of filtering and change logs
- regular review of filtering effectiveness
- taking part in reviews of the online safety policy and procedures
- ensure all governors and trustees receive appropriate online safety information/training as part of their safeguarding and child protection training

**Principal and SLT**

The Principal is responsible for ensuring the safety (including online safety) of members of the school community. Day to day responsibility for online safety will be delegated to the Online Safety Coordinator.

The Principal and Senior Leaders within the school are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. This training will be integrated into the wider safeguarding training.

The Principal and Senior Leaders will ensure that there are systems in place to allow for monitoring and support of those staff who carry out the internal online safety role.

The Principal and Senior Leaders will be aware of the procedures to be followed in the event of a serious online safety incident occurring.

The Principal and Senior Leaders oversee the safe use of electronic and social media by staff and take action immediately if they are concerned about bullying or risky behaviours.

The Principal and Senior Leaders will have an awareness and understanding of the filtering and other controls in place and will

manage them effectively while knowing how to escalate any concerns identified.

As part of the shortlisting process for new staff, SLT will ensure that an online search is carried out as part of the due diligence on shortlisted candidates to help identify any incidents or issues that have happened, and are publicly available online which the school might want to explore with applicants at interview

**Online Safety Coordinator**

The school will have a named member of staff with day to day responsibility for online safety. This role may be combined with the Designated Safeguarding Lead role. This is primarily a safeguarding role, not a technical role, although the coordinator should have a good understanding of technical issues.

The Online Safety Coordinator:

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies and documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority as appropriate
- liaises with IT technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Director of Education and Children's Services, NAS SGG to discuss current issues, review incident logs and filtering
- attends relevant meetings
- reports regularly to the Senior Leadership Team
- The Online Safety Coordinator will have an awareness and understanding of the filtering and other controls in place and will manage them effectively while knowing how to escalate any concerns identified.

**Staff**

All teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and procedures
- they report any suspected misuse or problem to the Online Safety Coordinator for investigation
- digital communications with pupils (for example by email or social networking) should be on a professional level
- online safety issues are embedded in all aspects of the curriculum and other school activities
- they help pupils understand and follow the school online safety and acceptable use policy
- they strive to ensure pupils have an understanding of behaving legally and responsibly online
- they monitor ICT activity in lessons, extracurricular and extended school activities
- they are aware of online safety issues related to the use of mobile phones, tablets, games machines, cameras and other devices and that they monitor their use and implement current school policies with regard to these devices
- they ensure that their own behaviour online is in accordance with professional standards, both within and beyond the school.
- The Designated Safeguarding Lead will have an awareness and understanding of the filtering and other controls in place and will manage them effectively while knowing how to escalate any concerns identified.

**Designated Safeguarding Lead**

Should be trained in issues relating to online safety and be aware of the potential for serious child protection/safeguarding issues that may arise from online activity such as:

- sharing of personal data
- access to illegal or inappropriate materials
- illegal or inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Designated Safeguarding Leads must be aware of online sexual harassment and how to deal with it. This may be standalone harassment, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

- consensual and non-consensual sharing of nude and semi-nude images and/or videos.140 Taking and sharing nude photographs of U18s is a criminal offence. UKCIS advice is available here: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- sharing of unwanted explicit content
- sexualised online bullying
- unwanted sexual comments and messages, including, on social media
- sexual exploitation; coercion and threats, and
- coercing others into sharing images of themselves or performing acts they're not comfortable with online.

**Pupils**

The school will attempt to give pupils the knowledge, skills and understanding to keep themselves safe online, both in the school and outside it.

Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to go about doing so. As far as possible Pupils will be expected to know and understand school policies on the use of mobile phones, tablets, games machines, cameras and other devices.

Pupils should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

**Parents/Carers**

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet in an appropriate way. The school are aware that parents and carers may not fully understand technical issues and be less experienced users of ICT than their children. Parents/carers often either underestimate or do not realise

how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what to do about it. The school will therefore take every opportunity to help parents understand these issues through collaborative working and training, which may include siblings or other family members as appropriate.

The school will work with parents to help them understand the systems in place to filter and monitor online usage, as well as engage parents/carers to reinforce the importance of their children being safe online.

Parents/carers are responsible for:

- working with the school to ensure that their children have the best opportunity to learn to keep themselves safe online
- signing the Pupil Acceptable Use Policy (if necessary)
- accessing the school's online resources in accordance with the relevant school policies

**IT Provider**

The IT provider is the NAS IT Department who manage a range of contractors and suppliers to provide It services.

The NAS IT Department has technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following incidents, concerns or checks to systems

The NAS IT Department will work with the senior leadership team and DSL to:

- procure, test, install and deploy systems
- identify risks and deliver mitigation
- carry out reviews to all systems

The NAS IT Department is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy to ensure that they carry out their work effectively in line with school policy
- the school technical infrastructure (including backend systems) is secure and is not open to misuse or malicious attack

- the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to school staff for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- monitoring systems are implemented and regularly updated as agreed in school policies

**Criteria for Success**

1. There is clear evidence that staff understand and act on the online safety policy. This may come from formal assessment of staff after training, review of incident logs and 'white hat' security testing. It is the responsibility of the Online Safety Coordinator to collect this evidence and of the Director of Education and Children's Services, NAS SGG to evaluate it.

2. Pupils are able to demonstrate increased understanding of online safety issues through formal and informal assessments.

3. Information on incidents show that they are being reported appropriately and that incidents are followed up.

4. This policy is reviewed and revised according to the set timescales.

**Procedures**

In line with previously published best practice there are three key aspects to online safety:

1. Education
2. Technical tools (e.g.: filtering, logging)
3. Review and revision of policy and procedure

To this we add inspection and monitoring as part of the support and 'friendly critic' role of senior managers.

While all three are intertwined in good practice, the school places great emphasis on the educational aspects, in particular because the technical tools may not always be present when a pupil is online (for example at home or in the community). The ability to stay safe online is something that pupils must be allowed to develop. This initially involves some degree of risk, however in the long term not giving pupils the skills to be safe online is likely to present an even greater risk. An analogy may be made with teaching independent travel and road safety: while there are very real, immediate and deadly risks involved in this, we still see the benefit of being safe on the road as being worth the risk in teaching those skills.

All pupils will therefore receive appropriate online safety education while at the school and this will be embedded into all aspects of the curriculum. Details of this can be found in the relevant curriculum documents.

The key skills that will be developed are:

- The importance of using technology safely and respectfully
- Understanding implications of sharing personal information
- Knowing where to go for help if they have concerns about content or contact on the internet
- Understanding the law as it applies online, in particular copyright and intellectual property rights.
- An awareness of the dangers and consequences of plagiarism, copyright infringement, piracy, and the reliability and bias of information sources.
- Understanding how to become a safe and responsible online citizen.
- How to develop positive, healthy and age appropriate online relationships

Responsibility for online safety is the responsibility of all members of the school. This means that education about online safety is the responsibility of all members of the school. The school actively encourages pupils to act as mentors to other pupils in many aspects of their education and in particular with regard to behaviour online. Mentors, cyber-buddies, e-pals and other input may come from pupils at the school or from vetted individuals from outside.

On admission to the school all pupils are assessed to see if they require an online safety plan. The purpose of this is to find out a pupil's online activity, likes and needs. The online safety plan will highlight support and education for the family and pupil around online safety issues. Not all pupils at our school require one.

**Dealing with online incidents**

All staff must be aware of pupils' use of online technologies. There are two essential things to look out for:

1. Pupils are encouraged to report anything that happens to them online that upsets them. This could range from something that is illegal (for example an attempt at sexual grooming, sexting, images of child abuse, financial embezzlement) through inappropriate behaviour (for example abusive behaviour online, bullying) to innocuous incidents that some people with autism may find distressing (for example being upset at a news story, seeing an image of a disliked food). It is crucial that all staff should be receptive to pupils and approachable to ensure pupils report when necessary. Staff should also be aware of the correct procedure to deal with pupils reporting incidents.

2. Pupils may not report an online activity that upsets them or which they know is wrong. This may be because they are not immediately aware of becoming upset or distressed, although their behaviour may indicate this. It may be that they perceive the 'upset' as 'normal'. It may be because they do not want to report it for any reason. Staff must be aware of behavioural, social or emotional indicators that a pupil has encountered something online that should be investigated.

When in doubt, any incident that causes concern should be reported to a line manager or the Online Safety Coordinator.

3. Cases of sexual violence and/or sexual harassment between children in can occur between children of any age and sex and may be one-to-one or many-to-one and can be in person as well as online. Children who are victims of sexual violence and/or sexual harassment are likely find it stressful, confusing and distressing. The effects are likely to be exacerbated if the alleged perpetrator(s) attend the same school. If a victim reports an incident follow the procedures laid out below.

Bear in mind also that safeguarding issues and abuse/neglect are rarely standalone events.

The following pages set out the procedures for reporting incidents in simple flow chart fashion:

Chart 1. Illegal activity online procedure

Chart 2. Inappropriate activity online procedure

Chart 3. Pupil as victim procedure

Chart 4. Illegal activities

**1. Illegal activity online procedure**

When an incident is reported staff (ideally the online safety coordinator and/or the Principal) will need to decide if the incident involved any **illegal** activity.

A list of illegal activities can be found in chart 4

If you are not sure if the incident has any illegal aspects – immediately report it anyway to the online safety coordinator, the Designated Safeguarding Lead or the Principal.

Was **illegal** material or activity found or suspected?

Yes

Inform police (**999)** and **Principal**/senior on site.

Follow the advice given by the police otherwise:

- Confiscate any computer or other device
- Power the device off at once. Do not shut it down as normal as this may remove evidence
- Lock the device away securely labelling it not to be touched
- If related to school network disable the user(s) account
- Save **any** evidence but **DO NOT** view or copy. Let the police review the evidence.

If a pupil is involved report using local safeguarding arrangements

If staff involved follow disciplinary procedures during police investigation (likely to involve suspension)

No

Follow the flowchart relating to **inappropriate incidents.**

## 2. Inappropriate activity online procedure



**The Online Safety Coordinator and/or Principal should:**

Record in the school safeguarding or online safety incident log and keep any evidence

**Incident** could be:

- Using another person's user name and password
- Accessing content which is against school policy
- Taking video without the subject's permission
- Using technology to upset or bully
  (in extreme cases this could be illegal – see illegal online activity procedure)

Did the incident involve a member of staff?

**Yes**

If member of staff has:

- Behaved in a way that has, or may have harmed a child
- Possibly committed a criminal offence
- Behaved towards a child in a way which indicates s/he is unsuitable to work with children…

**Contact the Principal**

- Review evidence and determine if the incident is accidental or deliberate
- Decide upon the appropriate course of action
- Follow school disciplinary procedures (if deliberate)

If the **Principal** is involved contact the **Director of Education and Children's Services**

**No**

Was the pupil the victim or the instigator?

**Pupil as victim**

Go to pupil as victim procedure

**Pupil as instigator**

- Review incident and identify if other pupils were involved
- Decide appropriate action based on school rules/guidelines/behaviour plan
- Inform parents/carers if serious or persistent incident
- In serious incidents consider informing the **Designated Safeguarding Lead** as the child instigator could be at risk
- Review online safety procedures/policies to develop best practice

**3. Pupil as victim procedure**

Incident assessed to consider who will need to take in-school action:

- Class teacher
- Safeguarding/online safety coordinator
- Senior leader or Principal
- Designated Safeguarding Lead

**Inappropriate image viewed by pupil(s)**

- Turn off monitor
- Isolate computer
- Ask another adult to look
- Provide appropriate opportunity for pupil(s) to talk about what they have seen.

**Unacceptable contribution to a webpage or forum online**

- Take a screen shot of contribution including the name of the contributor
- Delete (or ask pupil to delete) contribution
- Discuss contribution with pupil(s) involved as appropriate
- Action as appropriate according to school rules/behaviour plan

**Bullying contribution to a webpage or forum online**

- Take a screen shot of contribution including the name of the contributor
- Delete (or ask pupil to delete) contribution
- Take action according to the school's anti bullying policy

**Child safety concern about a contribution to a webpage or forum**

Report at once to Designated Safeguarding Lead

## 4. Illegal activities

**Illegal**

Child sexual abuse images: the making, production or distribution of indecent images of children. This may include images produced by a child of themselves (see: UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges

*The Protection of Children Act 1978*

Grooming, incitement, arrangement or facilitation of sexual acts against children

*The Sexual Offences Act 2003.*

Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). This includes images produced for sexual arousal which include: acts which threaten a person's life; an act which is likely to result in serious injury to the anus, breasts or genitals; a sexual act with a corpse; a sexual act with an animal; an act of non-consensual penetration.

*The Criminal Justice and Immigration Act 2008*

Criminally racist material in UK: material intended to stir up religious hatred (or hatred on the grounds of sexual orientation)

*The Public Order Act 1986*

Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to networks, data and files, through the use of computers or other devices
- Creating or propagating computer viruses or other harmful files

## Technical tools

The school filtering system (Netsweeper) is provided and managed at a technical level by the NAS IT Department. Configuration and specific filtering policy is set by the school through the Principal, DSL and online safety coordinator.

Filtering is applied at the network level and applies to any device connected to the school network, including BYOD. The system meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering (see appendix 1)

The filtering system allows different levels of access to different groups of users. Users are given more (or less) access depending on their ability to stay safe online. In this way the filtering of content is linked directly to pupils' learning. For example pupils may be given access to social networking sites as they have demonstrated that they are able to behave safely and responsibly on such sites.

Changes to filtering for these groups must be logged in the filtering log, as must changes to a pupil's level of access along with the reason for the change in access. The Online Safety Coordinator is responsible for these logs being kept accurate and up-to-date, although they do not have to be the person actually logging the information.

Alerts of inappropriate online behaviour can be generated and sent to key staff if requested by the school.

Logs of online activity are available on request from the NAS IT Department. These may be used to monitor and assess a pupil's online behaviour or to provide evidence in the case of an incident. Request for logs must be made through the Principal, DSL or the Online Safety Coordinator.

## Review and revision of policy and procedure

The Online Safety Coordinator has the leading role in reviewing the school online safety policies and documents. This process is overseen by the Principals and the Director of Education and Children's Services, NAS SGG.

Review will occur at least once a year and after a serious incident is recorded.

Review should take account of the following:

1. The effectiveness of the current policy and procedure

2. Changes to legislation

3. Advice on best practice from other agencies (e.g.: OfSTED) or tools such as SWGfL's 360 Degree Safe

4. The views of the whole school community. This includes pupils and parents/carers as well as other family members as appropriate.

## Appendix 1: Adherence to the 'Keeping Children Safe in Education' / UK Safer Internet Centre criteria

### Illegal content

IWF list and "police assessed list of unlawful terrorist content": blocked at source by the NAS Netsweeper product. To provide further protection the PaloAlto system that underpins our Wide Area Network is also an IWF licensee (see: https://www.iwf.org.uk/become-a-member/services-for-members/url-list/iwf-url-list-recipients for confirmation of current status).

Netsweeper is a direct partner of the Counter Terrorism Internet Referral Unit (CTIRU).

Logs allow identification of device IP address and (on main school network) the individual, the time and date of attempted access and search terms being blocked.

### Inappropriate Online Content

**Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.**

Covered by the Netsweeper category: Hate Speech

**Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances**

Covered by the Netsweeper category: Substance Abuse

**Extremism: promotes terrorism and terrorist ideologies, violence or intolerance**

Covered by the Netsweeper categories: Extreme, Hate Speech, Criminal Skills

**Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content**

Covered by the Netsweeper categories: Criminal Skills, Peer to Peer (i.e.: Child-on-Child), Infected Hosts. Malware is blocked at source by the NAS systems.

**Pornography: displays sexual acts or explicit images**

Covered by the Netsweeper category: Pornography

**Piracy and copyright theft: includes illegal provision of copyrighted material**

Covered by the Netsweeper categories: Criminal Skills, Peer to Peer (i.e.: Child-on-Child), Infected Hosts

**Self Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)**

Covered by the Netsweeper category: Extreme (specifically this will block self-harm sites, anorexia, bulimia and other content that can prove harmful to children).

**Violence: Displays or promotes the use of physical force intended to hurt or kill**

Covered by the Netsweeper category: Extreme

**Filtering System Features**

**Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role**

The school can provide this through Pupil logins or by access to different wireless SSIDs with different levels of filtering on each.

**Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content**

Control is delegated to the school. Staff can change filters themselves. Different sites can have different filtering policies to permit or deny access to specific content. Support, advice and emergency changes can be made by the NAS IT Department.

**Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking**

Netsweeper publishes classification of filtering and categorises on the Netsweeper website as well as a view in real time of new content categorised. This can be found at: http://www.netsweeper.com

**Identification - the filtering system should have the ability to identify users**

All users who login and all devices on BYO can be identified.

**Mobile and App content – isn't limited to filtering web traffic and includes the blocking of inappropriate content via mobile and app technologies**

The Local Area Network includes Application Visibility and Control which allows the blocking of mobile and app technologies.

**Multiple language support – the ability for the system to manage relevant languages**

The system supports the following languages: Arabic, English, French, German, Japanese, Persian, Polish, Russian, Chinese, Spanish, Turkish, Vietnamese, Italian, Portuguese, Romanian, Filipino, Korean, Catalan, Dutch, and Hungarian.

**Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices**

All filtering is done at the network level (LAN and WAN). There is no software on users' devices.

**Reporting mechanism – the ability to report inappropriate content for access or blocking**

Any member of staff can ask the local school technician or the central IT Department to block content who then escalate to our network provider.

**Reports – the system offers clear historical information on the websites visited by your users**

Demand and scheduled reports are available, in graphical or text format across a wide range of predefined or custom designs.

## Appropriate Monitoring

**Physical Monitoring**

This is used extensively across our schools as many of Pupils have intense on-to-one throughout the day and staffing levels often allow this.

**Internet and web access**

Regardless of whether physical monitoring is possible, weblogs monitor access and searches allowing staff to check for inappropriate behaviours and track usage.

**Active/Pro-active technology monitoring services**

The NAS is trialling the Impero Education Plus system to evaluate this as an active monitoring system. If suitable this can be made available to school where it is felt appropriate.

**Monitoring Content**

See above

## Appendix 2: Home learning guidance

For a number of reasons pupils may need to be educated at home. Should this be the case then NAS schools need to carefully consider how they will provide online resources. The schools' safeguarding teams should be involved in the overall planning of the school online learning approach.

Online learning can be either passive or active:

Passive: resources are sent to the pupil and they complete and send work back
Active: staff engage online with the pupil directly using video and audio. This may be with one pupil or with a group of pupils. Schools are strongly advised to have two members of staff on any active session

Recording a video lesson and sending it to a pupil is considered passive as there is no live interaction.

In considering how to proceed the ability of the pupil and the degree of support they will need should be taken into account. In our schools it is unlikely that there will be a single approach that works best and our person-centred approach is crucial here. In addition, staff competence to provide online education must be considered.

All NAS schools have an online education system (Teams for Education or Google Classroom) set up and centrally managed and supported. All online education must be provided through these platforms to ensure a proper audit trail, security and sustainability. Under no circumstances should active online learning take place outside these platforms. NAS provided devices should be used by staff when undertaking active online learning – personal devices must not be used.

Home based online learning activities must be planned carefully to take account of the home situation. Our schools have extensive filtering and safeguarding systems in place these are unlikely to be replicated in the home environment. Also be careful that pupils and their families do not incur unexpected costs through online learning, for example mobile data access charges as video uses significant amounts of data.

If live video and audio is being used, staff should think carefully about the location used at both ends. For example, pupils or staff being in their bedrooms may not be appropriate, even if the only available quiet space in crowded homes. The use of background effects to mask the location should be carefully considered.

Recording of any active session can only be made with the permission of school SLT and the pupil/parent/carer involved.

All existing safeguarding policies and procedures apply when home based online learning is in operation. Reporting lines and procedures remain the same.

Further advice is available from the DfE at:

https://get-help-with-remote-education.education.gov.uk/safeguarding

## Appendix 3: Legislation

The following appendix lays out some of the legislative framework under which this Online Safety Policy has been produced.

Note that, in most cases, an action that is illegal if committed offline is also illegal if committed online. For this reason not all laws are covered here, only those that specifically relate to online behaviour.

### Computer Misuse Act 1990

This Act makes it an offence to:

Erase or amend data or programs without authority;

Obtain unauthorised access to a computer;

“Eavesdrop” on a computer;

Make unauthorised use of computer time or facilities;

Maliciously corrupt or erase data or programs;

Deny access to authorised users.

### Data Protection Act 2018

This updated the 1998 Act and incorporated the General Data Protection Regulations (GDPR). The Act:

Facilitates the secure transfer of information within the European Union.

Prevents people or organisations from holding and using inaccurate information on individuals. This applies to information regarding both private individuals or businesses.

Gives the public confidence about how businesses can use their personal information.

Provides data subjects with the legal right to check the information businesses hold about them. They can also request that the data controller destroys it.

Gives data subjects greater control over how data controllers handle their data.

Places a greater emphasis on accountability. This requires businesses to have processes in place that demonstrate how they’re securely handling data.

Requires businesses to keep people’s personal data safe and secure and ensure that it is not misused.

Requires the data user or holder to register with the Information Commissioner.

In addition all data subjects have the right to:

Receive clear information about what their data is used for.

Access their own personal information.

Request that their data to be revised if out of date or erased.

Request information about the reasoning behind any automated decisions, such as if computer software denies them access to a loan.

Prevent or query about the automated processing of their personal data.

**Freedom of Information Act 2000**

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

**Communications Act 2003**

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

**Malicious Communications Act 1988**

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

**Regulation of Investigatory Powers Act 2000**

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

Establish the facts;

Ascertain compliance with regulatory or self-regulatory practices or procedures;

Demonstrate standards, which are or ought to be achieved by persons using the system;

Investigate or detect unauthorised use of the communications system;

Prevent or detect crime or in the interests of national security;

Ensure the effective operation of the system.

Monitoring but not recording is also permissible in order to:

Ascertain whether the communication is business or personal;

Protect or support help line staff.

The school reserves the right to monitor its systems and communications in line with its rights under this act.

### Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission.

### Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

### Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

### Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which

is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

### Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

### Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice including by phone or using the Internet. It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, that they are in a position of trust with. (Typically, teachers, social workers, health professionals, fall in this category of trust). Any sexual intercourse with a child under the age of 13 is an offence of rape.

### Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

### Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

**Human Rights Act 1998**

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

The right to a fair trial

The right to respect for private and family life, home and correspondence

Freedom of thought, conscience and religion

Freedom of expression

Freedom of assembly

Prohibition of discrimination

The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

**The Education and Inspections Act 2011**

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

**The Protection of Freedoms Act 2012**

Requires schools to seek permission from a parent / carer to use Biometric systems

**Serious Crime Act 2015**

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

**Criminal Justice and Courts Act 2015**

Revenge porn – as it is commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are

accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

### Counter-Terrorism and Border Security Act 2019

This act:

Creates an offence of reckless expressions of support for a proscribed organisation

Creates an offence of publication of images, and a police power to seize items as evidence, related to a proscribed organisation

Creates an offence of obtaining or viewing terrorist material over the internet

Creates an offence of entering or remaining in a designated area

Amends the offences of encouragement of terrorism and dissemination of terrorist publications

Extends extra-territorial jurisdiction for certain offences including inviting support for a proscribed organisation

Increases maximum sentences for terrorism offences

Makes extended sentences available for terrorism offences – ending automatic early release and allowing a longer period on licence

Strengthens notification requirements on convicted terrorists, and introduce greater powers to enter and search their homes

Extends Serious Crime Prevention Orders for terrorism offences

Provides for a statutory review of Prevent

## Guidance

### Ofsted (August 2015, updated 10 October 2018)

### Inspecting safeguarding in early years, education and skills settings

Embeds online safety in the inspection process for schools

### NSPCC training and guidance

https://learning.nspcc.org.uk/training/introductory/keeping-children-safe-online-online-course/

### Harmful online challenges and online hoaxes

https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes