Online Safeguarding Policy

(Incorporating mobile phone policy)

AUGHTON TOWN GREEN PRIMARY SCHOOL

Policy Creation and Review

This Online Safeguarding Policy has been written as part of a consultation process involving the following people:

Head Teacher: Mr N Huxley

Deputy Head/DSL: Mrs C Dykes

Online Safeguarding Leader: Mr A Gordon

This policy will be reviewed on a regular basis by:

Head Teacher: Mr N Huxley

Deputy Head/DSL: Mrs C Dykes

Online Safeguarding Leader: Mr Gordon

Contents

Appendices

1. Our vision for Online Safeguarding

Online Safeguarding at Aughton Town Green is a priority and whilst we want to encourage the pupils to use a diverse selection of modern technology to further their progress and enjoyment we have a duty to ensure that the children use technology in a safe manner.

Many of the aspects of Online Safeguarding fall outside school's parameters however, it is essential that the children in our care are given the tools they need to use advancing technology safely.

Maximising opportunities is a fundamental element in Aughton Town Green's Mission Statement, technology is key to progress and enjoyment and, at Town Green, we want to maximise the benefits and opportunities computing has to offer.

The children's learning environment must be secure; hence, we equip the pupils with the skills and knowledge to use not only the technology available in school but the technology that is widely available to children outside school, appropriately and responsibly. We feel it vital to work with parents and carers in their roles in encourage the safe use of technology.

2. The school's Online Safeguarding Leaders

At Town Green we acknowledge the importance of school representatives from the school community. The DSL and Online Safeguarding Lead will be a point of contact for Online Safeguarding related issues.

Designated Online Safeguarding Leader:

Mr A. Gordon

Designated Safeguarding Lead:

Mr N. Huxley
Mrs C. Dykes

The designated Safeguarding Leads have ultimate responsibility for all areas of online safeguarding (KCSIE2021) In Town Green the DSLs and Online Safeguarding Lead work closely as a team to provide the best possible online safeguarding for our pupils.

The role of the Online Safeguarding Leader should include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safeguarding Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an Online Safeguarding incident occur.
- Ensuring an Online Safeguarding Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with Online Safeguarding issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging Online Safeguarding advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's DSL to ensure a co-ordinated approach across relevant safeguarding areas.

3. Security and data management

In Town Green, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Secure data is available to staff at the discretion of the Head Teacher.

- Only the Head Teacher and Office Manager has remote access to secure Data.

- Staff are permitted to use removable devices such as: portable hard drives and cameras. Staff are asked to be vigilant when using such devices remotely and must not take any confidential data outside of the school building.

- Confidential data is stored securely only on the SLT drive or SIMs. SIMs cannot be accessed without passwords which are known only to the Head and Deputy and Office Manager. The SLT drive is only accessible to the Head and Deputy.

- Data is backed up on the Office and SLT drive to ensure data is not lost. SIMs is backed up remotely on a daily basis.

4. Use of mobile phones (Incorporating Mobile Phone Policy)

In Town Green we recognise the use of mobile devices offers a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

Mobile phones

- Staff should never give their mobile phone number to any pupils. This also includes past pupils under the age of 18 years.

- Staff should exercise caution when giving their mobile number to parents as this could be misconstrued. The school is aware that some staff members are also parents at the school. This is referred to in the school Code of Conduct Policy.

- Trips and Visits Offsite: The staff members in charge may use their mobile phones during visits offsite and when responsible for children away from school, to communicate arrangements to parents or colleagues or for emergency purposes. Should Staff need to use their mobile phone for personal use, which is acceptable on residential or extra-curricular activities, best practice is that mobile phones, wherever possible, should not be used in the presence of children.

- Staff are allowed to bring personal mobile phones into school. They must ensure the device is password protected.

- Staff are permitted to bring their phones into the classroom but they must be on 'silent' and may not be accessed during lesson time unless special permission has been granted by the Head Teacher.

- Staff are not permitted to use personal mobile phones to take photographs or videos of school related activities.

- Permission has been granted by the Head Teacher for staff to use their personal mobile phones to access music for curriculum related activities. Staff must ensure that all music being played is suitable for the age range being taught.

- Staff, volunteers and visitors will not use mobile phones in toilets or changing rooms accessible by pupils.

- Pupils are not permitted to bring mobile phones to school unless special arrangements have been made. In these cases the following procedures takes place:

1. **Pupil's mobile phone will be kept with the class teacher after being switched off by the pupil.**
2. **The phone will be kept in a secure place.**
3. **The phone will be returned to the pupil at the end of the day.**
4. **The pupil should only switch their phone back on once they have left the schools grounds.**
5. **If pupils need to contact their parents during the school day, this will be done through the school office as normal school procedures.**

This section of the policy will be displayed on the Safeguarding Board in the staffroom shared with the pupils and discussed at new staff/volunteer inductions.

IPads

- iPads must remain in school at all times unless permission is given by Head Teacher/Computing Lead
- iPads must be returned to the secure storage when not in use.
- Images and videos taken using the iPads should only be downloaded to the school server or can be added to Classdojo.
- The Computing Lead will have overall control of downloaded apps using MDM.

Laptops

- Staff laptops can be taken home.
- Staff are aware of the responsibility they have to ensure all content on these devices is legal and appropriate for a school setting.
- All laptops will be password protected and staff made aware of the importance of changing passwords on a regular basis.

5. Use of digital media (cameras and recording devices)

In Town Green we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance below.

- Only children with parental consent may appear in media pertaining to the school – newspaper articles/photos, website articles/photos, newsletters.
- Parental consent is requested by all parents on admission to the school. The wishes of those parents who choose not to consent are adhered to. **(See Appendix 1)**
- School may retain images of past pupils on the secure server or school website until such a time that it is updated or deleted.
- Full names and personal details will not be used in conjunction with any digital media, particularly in association with photographs.

- Parents and carers are permitted to take photos/videos of their own children in school (for example following assemblies, during sports days)
- Parents are asked not to publish any photos taken during school events on social networking sites as they may not have the permission of the parents of the pupils in the image. It is the responsibility of the parents to ensure that their child/children do not share these images on any other social media profile. ***(See Appendix 1 – Consent Form)***
- Mobile phones and cameras must not be used in pupil toilets or changing areas.
- Staff are not permitted to publish any school related photos on social networking sites apart from the school Twitter page/website/Classdojo.
- Staff must only use the school camera to take photographs of the children. These devices must not be taken outside of school unless permission is granted by the head teacher i.e. school extra-curricular activities and a residential. At the end of the school year staff must ensure that all images stored on the class camera are deleted.
- The Code of Conduct and/or Acceptable Use **(See Appendix 3,4,5)** /Behaviour Policy will outline when and where staff, volunteers and visitors can use their mobile phones.

6. Communication technologies

Email

In Town Green the following statements reflect our practice in the use of email:

- All teaching and non-teaching staff have access to their own Lancashire e-mail account. This is the preferred school e-mail system.
- Only official school e-mail addresses should be used to contact staff.
- The risk of SPAM is enormous when using external e-mail accounts, SPAM can often contain unsuitable material and viruses, and therefore, children are not permitted to access their external e-mail accounts in school.
- Staff are asked to be vigilant when accessing external e-mail accounts in school and should do so only when essential.
- Staff are reminded that it is essential to use safe practice when sending data via e-mail from school. E-mails are covered by the GDPR and school Privacy Notice.

Social Networks

In Town Green the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- School use 'Netsweeper Filtering' hence, social networking sites are blocked on all school computers.
- Children do not have any access to social media sites whilst in school. Regular updates are given to parents regarding age appropriate sites.
- All members of staff are given regular reminders and support around the use of social media. All staff adhere to the school social media policy which is also discussed and given out at new staff/volunteer induction.

- Pupils using social networking sites outside of school with permission of their parents are reminded of the safe usage of them. This is taught through our online safeguarding curriculum.
- Staff should not accept pupils or ex pupils younger than 18 as their 'friends'. They are encouraged not to accept parents as 'friends'. We are aware that some members of staff are also parents at our school and therefore is this circumstance is at the discretion of the member of staff.
- Staff should not engage in any discussion, via social networking, regarding school matters.

Text Messaging

In Town Green the following statements outline what we consider to be acceptable and unacceptable use of Text Messaging:

- Staff are permitted to use Text Messaging; however, this must only take place when a room is not being used by children or at inappropriate times.
- School iPads are not to be used for Text Messaging.
- The school uses Tucasi Messaging Service to contact parents. This can be accessed remotely by SLT in case of emergency or school closure. All text messages to parents would usually be sent out by the school office.

Video Conferencing – Zoom, Teams

In Town Green the following statements outline what we consider to be acceptable and unacceptable use of Video Conferencing:

- Video Conferencing is occasionally used at Town Green.
- Children will not be allowed to use a web camera without the presence of a member of staff.

School Website/Twitter

In Town Green the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

- All staff are made aware of the safe publication of media on the school website and Twitter. As below:
    1. Photographs of pupils can be uploaded to the website/Twitter but no names should be included
    2. At the start of the new academic year, all images of children should be deleted from the class pages.
    3. Staff should be aware of any children whose permission has not been received and ensure that no images of those children are included in the school website or Twitter page.
- The Head Teacher, The Office Manager and Staff have access through passwords to edit the school website.
- Any downloadable documents available on the school's website (Newsletters) will be available in 'read only' format, to prevent the content being manipulated.
- The school website contains a link to Online Safeguarding websites and to the relevant policy documents.

7. Infrastructure and technology

As Town Green use LEDS (Lancashire Education Digital Services), the internet content available to staff and pupils is filtered by default. Anti-Virus is also used on all school computers and regular updates are received. The Computing Lead/Online Safeguarding lead will carry out filter checks throughout the year to ensure the filter is providing appropriate protection.

Pupil's Access

All pupils are permitted access to the internet and through Online Safeguarding lessons are taught how to use this safely and appropriately. Any inappropriate use will result in appropriate sanctions being taken.

Pupils can only access certain areas of the network.

Adult Access

Staff will be restricted to certain areas of the school network. Staff will only be able to access their own user area and have personal login details.

Student Teacher Access

When students on placements attend, they are will not be permitted to use their own laptops unless it has been security checked by the Technician. They will also access the school network by logging in as a guest.

Passwords

In Town Green pupils and staff have to log onto the network using username and a password. The administrator of the network/class teacher has sole access to the pupil's passwords. The office and Head/Deputy Teacher's systems are password protected.

The following guidelines are used to ensure appropriate use of passwords:

- Staff must not display any passwords on their laptops or in classrooms.
- Staff are asked to change their passwords regularly.
- All staff and pupils are reminded regularly of the importance of keeping passwords safe and secure.
- Staff passwords must include a mixture of letters and numbers
- Pupils in KS1 have a password consisting of a four letter word and a number. Pupils in Years 3-6 have individual passwords.

- Pupil passwords will be changed at the start of every school year

Software/hardware

School has legal ownership of all hardware and software. Licenses are kept in a secure place. The subject leader audits the software and equipment. The Technician controls the installation of the software onto the server.

Managing the network and technical support

In Town Green we are aware that a safe network is required to ensure staff and pupils can work effectively. In order to ensure can happen the following procedures are used:

- The server, the wireless system and the cabling are all restricted.
- The technician has access to all the above.
- All wireless devices are security enabled.
- The Technician manages the school network system.
- Staff and pupils are asked to log out of their system once they have finished.
- The Technician will ensure that security of the server is kept up to date.
- Staff are not permitted to download online software at home.
- Pupils are not permitted to bring external drives into school. Any documents from pupils should be emailed to the school office.
- Staff can access the school network remotely.
- If staff use their laptop at home they are aware of appropriate use and dangers of infections being brought into school.
- The subject leader liaises with the Technician on a weekly basis.

Filtering and virus protection

- Town Green uses Netsweeper Filtering – BTLancashire Services filtering. **(See Appendix 9- Appropriate Filtering for Settings)**
- All staff are aware of the procedures for reporting suspected or actual virus infection. This should be recorded in the Technician's log book and reported verbally in the first instance to the Online Safeguarding Lead.
- The Technician will keep a weekly log of any inappropriate online use and this log will be passed to the Online Safeguarding Leader to investigate. If further action is needed this will be discussed with the DSL and SLT. Any incidents will be logged.

8. Dealing with incidents

All incidences of inappropriate use will be logged on a green incident sheet by the reporting member of staff and passed on to the Online Safeguarding Lead. **(See Appendix 11)** Following the procedures flowchart **(See Appendix 12),** if necessary, the incident will be escalated to the DSL. Further monitoring of the incident will take place by the DSL/Head teacher working in conjunction with the Online Safeguarding Lead. All incidents will be reported to the SLT during each SLT meeting. Governors

will receive this information through the termly Head Teacher's report. All incident sheets will be stored in a folder which will be kept securely in the Head's office.

Any suspected illegal offences should be brought to the attention of the Head Teacher and DSL and dealt with immediately using the procedures flowchart.

Inappropriate use

At Town Green we aim to ensure all staff and pupils can work in a safe environment and are aware that on occasions rules may be broken. The following procedures and sanctions are used to address any incidents of misuse:

Accidental access to inappropriate materials:

- Minimise the webpage/turn the monitor off
- Tell a trusted adult.
- Enter the details in the Incident Log and report to LGfL filtering services if necessary.
- Persistent 'accidental' offenders may need further disciplinary action.

Using other people's logins and passwords maliciously.

- Inform DSL and designated Online Safeguarding Lead.
- Enter the details in the Incident Log.
- Additional awareness sessions of Online Safeguarding issues and the AUP with individual child/class.
- More serious or persistent offences may result in further disciplinary action in line with Behaviour Policy.
- Consider parent/carer involvement.

Deliberate searching for inappropriate materials:

- Inform DSL and designated Online Safeguarding Lead.
- Enter the details in the Incident Log.
- Inform parent/carer involvement and appropriate action following Behaviour Policy guidelines. (Unacceptable Behaviour)

Bringing inappropriate electronic files from home:

- Inform DSL and designated Online Safeguarding Lead.
- Enter the details in the Incident Log.
- Inform parent/carer of the incident
- Contact appropriate services if more serious.

Staff know how to report an incident to DSL/Online safeguarding lead. **Online Safeguarding Concern Log. (See Appendix 11)**

Staff and parents are made aware of the procedures to follow in the case of an online incident. **Responding to incidents and misuse (See Appendix 12)**

9. Acceptable Use Policy (AUP)

Staff, pupils and parents are asked to sign an AUP. Parents are asked to sign when their children are admitted to the school, pupils are asked to sign when they reach KS2 and staff are asked to sign when they commence work at Town Green. The children and staff are reminded of the AUP annually. **(See Appendix 3, 4 and 5)** A letter to parents will be sent out explaining the requirement of the AUP. **(See Appendix 6)**

10. Education and training

At Town Green we are aware that adults and children need to be digitally literate and aware of the benefits that use of technology can provide. However, we realise it is essential that children are taught to use technology responsibly, securely and safely, being able to recognise potential risks and knowing how to respond.

The four areas of Online Safeguarding risk (as mentioned by KCSIE, 2022) that we make our pupils and staff aware of and consider are:

• **Content**: - being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti- Semitism, radicalisation, and extremism.

• **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• **Conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

• **Commerce**: risks such as online gambling, inappropriate advertising, phishing and financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

Online Safeguarding - Across the curriculum

In the 21st Century society, staff and pupils need to be digitally literate and aware of the benefits that the use of technology can provide. However, it is essential that pupils are taught to be responsible and safe users of technology, being able to recognise potential risks and knowing how to respond.

Online Safeguarding – Raising Pupil's awareness

- Online Safeguarding is taught from the Foundation Stage to Year 6 during lessons, assemblies, PSHE and by following the Rising Stars 'Switched on' Online Safeguarding Scheme. See curriculum map
- Online Safeguarding will be differentiated through support for pupils with SEN.
- Pupils are reminded annually of the AUP and their own responsibility to act safely both inside and outside school.
- Each classroom has a 'Golden Rules' poster. This reminds the children about their online responsibilities and what to do if they are concerned about something that has happened online. **(See Appendix 7,8)**

Online Safeguarding – Raising staff awareness

- Staff will receive INSET training and staff meeting training on Online Safeguarding.
- Staff are asked to sign and AUP regarding social networking and are advised of the impact social networking can have on their personal safeguarding and professional conduct.
- New staff are asked to sign the AUP and an induction is carried out by the DSL.
- Updates at staff meetings on Online Safeguarding and AUP are held when necessary.

Online Safeguarding – Raising parents/carers awareness

"Parents 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 they would do about it." (Byron Report, 2008).

- Online Safeguarding will be addressed to parents via letters, workshops **(See Appendix 10),** the School's website or Twitter page.
- Parents will be pointed in the direction of Online Safeguarding resources and online materials on the website.
- Parents will be updated on Online Safeguarding matters within school.

Online Safeguarding – Raising Governors' awareness

- Governor will be invited to attend any Online Safeguarding meetings/evenings/INSET
- The Online Safeguarding Policy will be reviewed regularly and approved by the governing body.

- Online Safeguarding will be discussed during curriculum committee meetings.

The Online Safeguarding Leader will keep a log of all the training that takes place.

11. Evaluating the impact of the Online Safeguarding Policy

At Town Green we recognise the importance of monitoring the impact of safeguarding procedures throughout school. In order to ensure the impact is positive and continuous the following procedures will be followed:

- Incidents will be analysed by the SLT to see if there is a recurring pattern.
- Policy and AUP will be amended if new devices are deemed to pose a risk.
- Governors and staff will be informed of any updates to the policy.

Appendices

APPENDIX 1

Aughton Town Green Primary - Pupil Data Collection Form

This information will be used on a computerised system. The school is registered under the Data Protection Act to keep such information.
Pupil data will be used for statutory returns to the Local Authority and registered Government Agencies.

PUPIL PERSONAL INFORMATION

LEGAL SURNAME		**PREFERRED SURNAME**	
LEGAL FORENAME		**PREFERRED FORENAME**	
MIDDLE NAME(S)		**GENDER**	Male / Female
BIRTH CERTIFICATE SEEN?		**DATE OF BIRTH:**	____/____/ _____
HOME ADDRESS **including post code**			

PARENT INFORMATION

*** Please indicate at which address(es) the pupil normally resides (i.e. sole or shared residency) using the tick box**

MOTHER

TITLE		**FORENAME**		**SURNAME**	
DATE OF BIRTH		**PARENTAL RESPONSIBILITY**		Yes / No	
HOME ADDRESS **including post code**	*				
TELEPHONE NUMBERS		**HOME:** **MOBILE:**		**WORK:**	
E-MAIL ADDRESS					

FATHER

TITLE		**FORENAME**		**SURNAME**	
DATE OF BIRTH		**PARENTAL RESPONSIBILITY**		Yes / No	
HOME ADDRESS **including post code**	*				
TELEPHONE NUMBERS		**HOME:** **MOBILE:**		**WORK:**	
E-MAIL ADDRESS					

If there is any other person who can be deemed a 'parent' (eg. step parent, or parent's partner) if so please provide their details below, indicating if they have 'parental responsibility', continue on a separate sheet if necessary.

TITLE		**FORENAME**		**SURNAME**	
DATE OF BIRTH		**RELATIONSHIP TO CHILD**		**PARENTAL RESPONSIBILITY**	Yes / No
HOME ADDRESS **including post code**	*				
TELEPHONE NUMBERS		**HOME:** **MOBILE:**		**WORK:**	

This information will be used on a computerised system. The school is registered under the Data Protection Act to keep such information. Pupil data will be used for statutory returns to the Local Authority and registered Government Agencies.

CONTACT INFORMATION – IN PRIORITY ORDER Attach an extra sheet if necessary

Please provide below the names of at least two people who can be contacted by school in emergency, underlining the main contact number. (Attach information on an extra sheet if necessary)

Texts will be sent to 1st Contact No.

TITLE		**FORENAME**		**SURNAME**	
Address (including postcode)			this no. will be used for text messaging service		
HOME:		**WORK:**		**MOBILE:**	
RELATIONSHIP TO CHILD					

Contact 2

TITLE		**FORENAME**		**SURNAME**	
Address (including postcode)					
HOME:		**WORK:**		**MOBILE:**	
RELATIONSHIP TO CHILD					

Contact 3

TITLE		**FORENAME**		**SURNAME**	
Address (including postcode)			this no. will be used for text messaging service		
HOME:		**WORK:**		**MOBILE:**	
RELATIONSHIP TO CHILD					

MEDICAL/DIETARY INFORMATION – Attach an extra sheet if necessary

NAME OF DOCTOR:		**NAME AND ADDRESS OF PRACTICE:**	
MEDICAL CONDITIONS:			
ANY SPECIAL DIETRAY			

ETHNICITY		**RELIGION**	
HOME LANGUAGE		**FIRST LANGUAGE**	

TRAVEL ARRANGEMENTS	**BICYCLE/TRAIN/CAR/WALK/TAXI/ OTHER**	

Please indicate if any of the following areas are relevant. All information collected is strictly confidential. The school may receive additional funding which can be used to support your child's learning further.

SERVICE CHILDREN IN EDUCATION	YES/NO	**ADOPTED FROM CARE**	YES/NO
ENTITLED TO PUPIL PREMIUM & FREE SCHOOL MEALS pupils in reception, year 1 or year 2 are entitled to free school meals but if you are eligible for benefits, our school will receive additional funding to further support your child..	YES/NO If yes please apply to your local authority or contact the school office	**LOOKED AFTER CHILD**	YES/NO

PREVIOUS SCHOOL / NURSERY INFORMATION – IF APPLICABLE (use extra sheet if necessary)

Previous School, Nursery etc			
From	/ /	**To:**	/ /

Parental Consent

EMERGENCY/ACCIDENT/ ILLNESS	**In the case of any emergency Aughton Town Green Primary have the right to take such actions as are deemed necessary**	*Please Sign
SCHOOL OUTINGS	**I agree for my child to participate in local outings from school, for trips involving transport you will receive a further trip letter**	* Please Sign
SCHOOL PHOTOGRAPHS/ RECORDINGS	**I give permissions for my child's photograph to be used in School Publications/Local Press/Website/Twitter and recordings, no names will be attached.**	* Please Sign
SCHOOL INTERNET POLICY	**I give permissions for my child to access the internet in school via appropriate websites in accordance with the school Computing & online Safeguarding policies (for more information see the school website)**	* Please Sign
PRIVACY NOTICE	**I have read the Privacy Notice**	*Please Sign

PLEASE NOTE ANY PERSONAL INFORMATION MAY BE SHARED IN ACCORDANCE WITH DATA PROTECTION LAW

Signature _____ **Date** _____

Name (please print) _____

Relationship to child: _____

APPENDIX 2
Consent Form for Images to be Taken e.g. A School Production or Special Event

Dear Parent/ Carer,

Your child will be appearing in our school production / event name on <*insert date/s*>. We are aware that these events are special for children and their relatives / friends and form treasured memories of their time at school.

We have a rigorous policy in place with regard to taking, using and publishing images of children and you have already signed a consent form stating whether you agree to your child's images / video being used in general circumstances.

Many parents / carers like to take photographs / videos of their children appearing in school productions, but there is a strong possibility that other children may be included in the images. In these circumstances, we request specific consent for images / videos to be taken by a third party (i.e. other parents). We need to have permission from all parents / carers of children involved in the production to ensure that they are happy for group images / videos to be taken and I would be grateful if you could complete the slip at the bottom of this letter and return to school as soon as possible.

We would also request that images / videos including other children or adults are not posted online, especially on Social Media sites e.g. Facebook without the specific permission of the individuals included in the footage.

Should any parents / carers not consent, we will consider other options, e.g. arranging specific photo opportunities after the production.

These decisions are not taken lightly, but we have to consider the safeguarding of all our children and respect parents' rights to privacy.

Yours sincerely,

Head teacher.

Child's name: _____ Date: _____
I agree / do not agree to photographs / videos being taken by third parties at the <*insert event*> *on*
<*Insert date /s*>.
Signed _____ *(Parent / Carer)*
Print name _____

APPENDIX 3

Computing Acceptable Use Policy (AUP) – Staff and Governors

Computing and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and Governors are aware of their individual responsibilities when using technology. All staff members and Governors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the head teacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.
2. I will be an active participant in Online Safeguarding education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.
3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.
4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, children or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.
5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.
6. I will respect copyright and intellectual property rights.
7. I will ensure that all electronic communications with children and other adults are appropriate.
8. I will not install any hardware or software without the prior permission of SLT.
9. I will ensure that personal data (including data held on SIMs) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.
10. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.
11. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.
12. I will report any known misuses of technology, including the unacceptable behaviours of

others.

13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures will come into action which may include contacting outside agencies

18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's Online Safeguarding Policy and help children to be safe and responsible in their use of computing and the internet.

19. I understand that these rules are designed for the safeguarding of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of computing and internet throughout the school.

Signature
.....
Date .....
Full Name
.....(PRINT)
Position/Role
.....

APPENDIX 4

Acceptable Use Policy (AUP) – Students, Supply Teachers, Visitors, Guests etc.

To be signed by any adult working in the school for a short period of time.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

3. I will not use any external device to access the school's network e.g. pen drive.

4. I will respect copyright and intellectual property rights.

5. I will ensure that images of children and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

6. I will abide by the school's rules for using personal mobile equipment, including my mobile phone, at all times.

7. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

8. I will not install any hardware or software onto any school system.

9. I understand that these rules are designed for the safeguarding of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature
I have read and agree to follow this code of conduct and to support the safe use of COMPUTING throughout the school.

Signature
.....

Date .....

Full Name .....
(PRINT)

Position/Role .....

Appendix 5

Acceptable Use Policy (AUP) - Children

These rules reflect the content of our school's Online Safeguarding Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using Computing, including use of the Internet.

- I will only use computing in school for school purposes.
- I will not bring equipment e.g. a mobile phone or mobile games consoles into school unless specifically asked by my teacher.
- I will only use the Internet and/or online tools when a trusted adult is present.
- I will only use my class e-mail address or my own school email address when emailing.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- I will not deliberately bring in inappropriate electronic materials from home.
- I will not deliberately look for, or access inappropriate websites.
- If I accidentally find anything inappropriate I will tell my teacher immediately.
- I will only communicate online with people a trusted adult has approved.
- I will make sure that all computing contact with other children and adults is responsible, polite and sensible.
- I will not give out my own, or others', details such as names, phone numbers or home addresses.
- I will not tell other people my computing passwords.
- I will not arrange to meet anyone that I have met online.
- I will only open/delete my own files.
- I will not attempt to download or install anything on to the school network without permission.

- I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
- I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safeguarding.
- I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

Parent/ Carer Signature
We have discussed this Acceptable Use Policy and
..... [Print child's name] agrees to follow the Online Safeguarding rules and to support the safe use of computing at *Aughton Town Green Primary School*.

Parent /Carer Name (Print) .....

Parent /Carer (Signature) .....

Date.....

This AUP must be signed and returned before any access to school systems is allowed.

APPENDIX 6

Acceptable Use Policy (AUP) – Parent's Letter

<Insert School's Letterhead>

Dear Parent/Carer,

The use of computing including the Internet, e-mail and mobile technologies are integral elements of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all children to act safely and responsibly when using technology both within, and outside of, the school environment.

In school, we ensure that all resources used by the children are age appropriate and suggest that parents check the terms and conditions for the use of online resources and games to ensure that resources used at home are also age appropriate. This is particularly relevant when using Social Network Sites that incorporate age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of the site's privacy policy and / or terms and conditions and therefore we actively discourage this in our school.

The enclosed Acceptable Use Policy forms part of the wider School Online Safeguarding Policy and
alongside the school's Behaviour and Safeguarding Policies outlines those principles we expect our children to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed Acceptable Use Policy with your child and return the completed document as soon as possible. Signing the School Acceptable Use Policy helps us to maintain responsible use of computing and safeguard the children in school.

Along with addressing Online Safeguarding as part of your child's learning, we will also be holding Parental Online Safeguarding Awareness Sessions during the school year and I would take this opportunity to strongly encourage your attendance wherever possible. Further information on these sessions will be communicated as soon as dates are confirmed. In the meantime, if you would like to find out more about Online Safeguarding for parents and carers,

please visit the Lancsngfl Online Safeguarding website http://www.lancsngfl.ac.uk/OnlineSafeguarding

If you have any concerns or would like to discuss any aspect of the use of computing in school, please contact <*insert school contact person*>.

Yours sincerely,

<*The Headteacher*>

APPENDIX 7
Typical Classroom Online Safeguarding Rules (KS1)

Our Golden Rules for Staying Safe with COMPUTING

We only use the Internet when a trusted adult is with us.

We are always polite and friendly when using online tools.

We always make careful choices when we use the Internet.

We always ask a trusted adult if we need help using the Internet.

We always tell a trusted adult if we find something that upsets us.

Trusted Adult: _____

APPENDIX 8
Typical Classroom Online Safeguarding Rules (KS2)

Our Golden Rules for Staying Safe with COMPUTING

We always ask permission before using the internet.

We only use the Internet when a trusted adult is around.

We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).

We always tell an adult if we see anything we are uncomfortable with.

We only communicate online with people a trusted adult has approved.

All our online communications are polite and friendly.

We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.

We only use programmes and content which have been installed by the school.

Trusted Adult: _____

APPENDIX 9

Appropriate Filtering for Education settings

June 2021

Filtering Provider Checklist Reponses

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering". Furthermore, the Department for Education's statutory guidance 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place*" and they "should be doing all that they reasonably can to limit*

children's exposure to the above risks from the school's or college's IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what

children can be taught with regards to online teaching and safeguarding."

Included within the Scottish Government national action plan on internet safety, schools in Scotland are expected to "have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content."

By completing all fields and returning to UK Safer Internet Centre (enquiries@saferinternet.org.uk), the aim of this document is to help filtering providers to illustrate to education settings (including Early years, schools and FE) how their particular technology system(s) meets the national defined 'appropriate filtering standards. Fully completed forms will be hosted on the UK Safer Internet Centre website alongside the definitions

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Company / Organisation	Netsweeper
Address	Suite 125-126 Pure Offices, 4100 Park Approach Thorpe Park, Leeds, United Kingdom, LS15 8GB
Contact details	Lou Erdelyi, lou.erdelyi@netsweeper.com
Filtering System	Netsweeper
Date of assessment	August 18, 2021

System Rating response

Where a supplier is able to confirm that their service fully meets the issue identified in a specific checklist the appropriate self-certification colour for that question is GREEN.	
Where a supplier is not able to confirm that their service fully meets the issue identified in a specific checklist question the appropriate self-certification colour for that question is AMBER.	

.

Illegal Online Content

Filtering providers should ensure that access to illegal content is blocked, specifically that the filtering providers:

Aspect	Rating	Explanation
• Are IWF members		Netsweeper is a Member of the IWF
• and block access to illegal Child Abuse Images (by actively implementing the IWF URL list)		Compliant
• Integrate the 'the police assessed list of unlawful terrorist content, produced on behalf of the Home Office'		Compliant

Inappropriate Online Content

Recognising that no filter can guarantee to be 100% effective, providers should both confirm, and describe how, their system manages the following content

Content	Explanatory notes – Content that:	Rating	Explanation
Discrimination	Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age, or sex.		Netsweeper has a category for this
Drugs / Substance abuse	displays or promotes the illegal use of drugs or substances		Netsweeper has a category for this
Extremism	promotes terrorism and terrorist ideologies, violence or intolerance		Netsweeper has a category for this
Malware / Hacking	promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content		Netsweeper has a category for this
Pornography	displays sexual acts or explicit images		Netsweeper has a category for this
Piracy and copyright theft	includes illegal provision of copyrighted material		Netsweeper has a category for this
Self Harm	promotes or displays deliberate self harm (including suicide and eating disorders)		Netsweeper has a category for this
Violence	Displays or promotes the use of physical force intended to hurt or kill		Netsweeper has a category for this

This list should not be considered an exhaustive list. Please outline how the system manages this content and many other aspects

Netsweeper integrates and consumes various lists as well as generate it's own database. Real-time content filtering ensures students always have the best protection. Netsweeper's AI-based

web content categorization platform is the industry's most accurate and effective solution to classify online content with over 90 categories and 50 languages.

Regarding the duration and extent of logfile (Internet history) data retention, providers should outline their retention policy, specifically including the extent to the identification of individuals and the duration to which all data is retained .

Netsweeper will maintain logfiles/history for as long as required or requested by the school.

Providers should be clear how their system does not over block access so it does not lead to unreasonable restrictions

The Netsweeper AI-powered platform provides on-the-fly categorization for all content that ensures detection of new and emerging safeguarding threats that is very accurate. Industry-leading database of over 3 billion URLs with real-time dynamic updates to education-specific categories including hate speech, weapons, cyberbullying, and substance abuse. Categories are populated dynamically by AI – they are not static lists. Categorization occurs in over 47 languages. Every Netsweeper deployment globally contributes to the platform with over 150 million URLs categorized every day. Should an over blocking occur, Administrators are able to easily update the system on their own or report such occurrences directly to Netsweeper for further analysis.

Filtering System Features

How does the filtering system meet the following principles:

Principle	Rating	Explanation
• Age appropriate, differentiated filtering – includes the ability to vary filtering strength appropriate to age and role		Users are sourced from the school's authentication system via grade.
• Circumvention – the extent and ability to identify and manage technologies and techniques used to circumvent the system, specifically VPN, proxy services and DNS over HTTPS.		Netsweeper has developed a decrypting SSL proxy that inspects all encrypted traffic including DoH.
• Control - has the ability and ease of use that allows schools to control the filter themselves to permit or deny access to specific content		Schools utilize a Web Administration system that allows schools to manage their policies and content.
• Contextual Content Filters – in addition to URL or IP based filtering, the extent to which (http and https) content is analysed as it is		Netsweeper has developed an AI system that can inspect content in multiple languages.

streamed to the user and blocked. For example, being able to contextually analyse text on a page and dynamically filter		
• Filtering Policy – the filtering provider publishes a rationale that details their approach to filtering with classification and categorisation as well as over blocking		Yes, Netsweeper publishes this information https://helpdesk.netsweeper.com/docs/7.2/Tech_Notes/CNS_Categorization.htm?rhhlterm=categorization https://helpdesk.netsweeper.com/docs/7.2/Quick_Overview/Categorization_Training/Dynamic_Content_Training.htm?rhhlterm=categorization
• Group / Multi-site Management – the ability for deployment of central policy and central oversight or dashboard		Netsweeper is built with this concept in mind and supports many different models including hub and spoke, central, distributed, etc.
• Identification - the filtering system should have the ability to identify users		Netsweeper can be integrated with a central authentication system such as LDAP, Azure AD, Novel, Google, Apple, etc, including the ability to statically map the user information.
• Mobile and App content – mobile and app content is often delivered in entirely different mechanisms from that delivered through a traditional web browser. To what extent does the filter system block inappropriate content via mobile and app technologies (beyond typical web browser delivered content)		Netsweeper is deployed as a network service which can detect applications protocols if the Netsweeper is also deployed to perform DPI.
• Multiple language support – the ability for the system to manage relevant languages		Netsweeper supports over 40 languages.
• Network level - filtering should be applied at 'network level' ie, not reliant on any software on user devices whilst at school (recognising that device configuration/software may be required for filtering beyond the school infrastructure)		Netsweeper is primarily a Network filtering solution with the ability to extend it's filtering reach via the use of Client Filter software installed on PC, MAC, Google Chrome, IOS and Android devices.

• Remote devices – with many children and staff working remotely, the ability for devices (school and/or personal) to receive school based filtering to a similar quality to that expected in school		Netsweeper can provide remote filtering if the student/staff devices is connected via VPN to the schools network unless the remote device has the Netsweeper Client Filter software installed which does not require a VPN connection.
• Reporting mechanism – the ability to report inappropriate content for access or blocking		Netsweeper provides a comprehensive suite of pre-defined reports as well as offer reporting on a custom level. Reporting can be done and managed by the ITC.
• Reports – the system offers clear historical information on the websites visited by your users		The Netsweeper system logs details of the user activity and then allows reports to be generated including a time line report that shows access over time.

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "*consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum*".[1]

Please note below opportunities to support schools (and other settings) in this regard

Netsweeper offers educational messaging to staff and students that can be used to further inform users of dangers.

[1] https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

PROVIDER SELF-CERTIFICATION DECLARATION

In order that schools can be confident regarding the accuracy of the self-certification statements,the supplier confirms:

- that their self-certification responses have been fully and accurately completed by a personor persons who are competent in the relevant fields
- that they will update their self-certification responses promptly when changes to the serviceor its terms and conditions would result in their existing compliance statement no longer being accurate or complete
- that they will provide any additional information or clarification sought as part of the self-certification process
- that if at any time, the UK Safer Internet Centre is of the view that any element or elementsof a provider's self-certification responses require independent verification, they will agree to that independent verification, supply all necessary clarification requested, meet the associated verification costs, or withdraw their self-certification submission.

Name	Lou Erdelyi
Position	CTO
Date	August 18, 2021
Signature	

APPENDIX 10
Letter to Parents Regarding Parental Online Safeguarding Awareness Session

<Insert School's Letterhead>

Dear Parent/Carer,

Having access to online information and the opportunities that the digital world can offer has many benefits and for some it plays an important part of our everyday lives. However, as technology moves on at such a pace, it is sometimes difficult to keep up with new trends and developments, particularly with regard to mobile/games technologies and secure and safe accessibility to online material.

Our school has policies in place to ensure our children are learning in a safe and secure environment which includes being safe online. This session has been organised to help you to contribute to the process of helping your child to be aware of the potential risks associated with using the Internet and modern technologies.

Ofsted increasingly view Parental Online Safeguarding Awareness sessions as essential components of effective safeguarding provision and I would therefore appreciate your support in attending this event.

We will be hosting the above session on the Date/Time below and I would strongly encourage your attendance:

Date:……..Time:……
……

The session will include reference to the following areas with time for you to ask questions:

- What are our children doing online and are they safe?
- Do they know what to do if they come across something suspicious?
- Are they accessing age-appropriate content?
- How can I help my child stay safe online?

The session will last for approximately 1¼ hrs where a member of the Local Authority Schools' Computing Team will address the issues mentioned above.

Yours sincerely,

<The Headteacher>

I / we will be attending the above Parental Online Safeguarding Awareness Session

Name(s):.....
.....

Parent / Carer of:.....
Year Group.....

APPENDIX 11
Online Safeguarding Concern Log

Pupil Name			**Class**		
Date			**Time**		
Reason for concern	*If applicable, please include location of computer or iPad number and record any website addresses.*				
Completed by		**Signature**		**Date**	
Received by		**Signature**		**Date**	
Action Taken					

Conclusion Feedback	

APPENDIX 12

Responding to Online Safeguarding Incident/ Escalation Procedures