Forest View Primary School

Digital Safety Policy

April 2021

Contents of this Policy:

Development / Monitoring / Review of this Policy

This Digital Safety Policy has been developed by a working group made up of:

- Headteacher - Mrs Cook
- Computing Coordinator - Miss Charlton
- DSL and Deputy DSL
- Governors
- ICT in Schools South Tyneside

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This Digital Safety Policy was approved by the Board of Directors / Governing Body / Governors Sub Committee on:	*January 2020* *Updated October 2020* *Updated April 2021*
The implementation of this Digital Safety Policy will be monitored by the:	*Headteacher* *Computing Coordinator*
Monitoring will take place at regular intervals:	*Annually*
The Board of Directors / Governing Body / Governors Sub Committee will receive a report on the implementation of the Digital Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Annually*
The Digital Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*Annually*
Should serious online safety incidents take place, the following external persons / agencies should be informed:	*LA Safeguarding Officer, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) / filtering by Esafe
- Surveys / questionnaires of
    - pupils
    - parents / carers
    - staff

Scope of the Policy

This policy applies to all members of Forest View's community (including staff, pupils, volunteers, parents / carers, visitors) who have access to and are users of school digital technology systems, both in and out of the school.

Our school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

The Digital Safety Policy is a complementary document that informs a suite of documents to ensure the safety of all of our digital technology users (pupils, staff, parents/carers, volunteers, visitors). The Digital Safety Policy is informed by Forest View's Computing Policy, Data Protection Policy, Safeguarding Policy, Behaviour Policy and PSHE Policy.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the *school:*

Governors

Governors are responsible for the approval of the Digital Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding.

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher is responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Designated Safeguarding Lead

The Designated Safeguarding Lead is trained in Online Safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

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

Technical staff

Forest View has a managed service which provides technical support, internet and broadband access, filtering and monitoring. This is provided by ICT in Schools and Durham Net.

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 Digital Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Digital Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying.
- should understand the importance of adopting good online safety practices when using digital technologies out of school and realise that the *school's* Digital 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 / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student / pupil records
- the use of social media sites

Policy Statements

Digital Citizenship – Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and events
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Forest View will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, our school website
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant websites

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in the use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Staff

Staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered periodically to keep staff up to date with technological advancements.

Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation
- Participation in school training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

Our school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements through the SLA with ICT in Schools Team.

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password..
- The "master / administrator" passwords for the school ICT systems, used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

- Technicians are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes - logging requests with the school office to be managed by ICT in schools team.
- Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering (allowing different filtering levels for different groups of users – staff / pupils / etc).
- Activity of users on the school technical systems is monitored and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet and G Suite for Education.

All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Our school will inform and educate users about these risks and implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before images of pupils are published on the school website / social media / local press.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other in the digital / video images.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with images.

Use of portable storage devices (drives and memory pens)

Forest View does not allow the use of portable storage unless by authorisation from the Head Teacher. Cloud storage is the preferred method.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation and Forest View's Data Protection Policy.

Staff must ensure that they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected systems.

Communications

Forest View allows:

	School Devices	Personal Devices		
	School owned for single user	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*No*	*No*	*No*
Internet only	*Yes*	*No*	*No*	*No*
No network access	*Yes*	*Yes*	*Yes*	*Yes*
Use of social media	*Certain staff*	*No*	*Yes*	*Yes*

Protecting Professional Identity

Our school and local authority have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.

- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that they follow the staff Acceptable Use Policy at all times.

Responding to incidents of misuse

Forest View follows the LA Reporting of Incidents as shown in Appendix ii.

Appendices

Appendix i) - Acceptable Use Policy Agreement

Appendix ii) - Responding to Incidents

Appendix iii) - Other Incidents

Appendix iv) - Using Video Conferencing and Virtual Lessons during School Closures - Covid-19

Appendix i)

Student / Pupil Acceptable Use Agreement Form

I will not use the computer without permission.

I will check with an adult before using Internet or email.

I will not give away any personal details, including passwords.

I will not click on email addresses shown on websites.

I will not download anything from the Internet without permission.

I will tell an adult if I see anything unpleasant.

I understand that the school may check my computer files and may monitor the Internet sites I visit.

I will not use my own disks or pen drives.

I know that all my communications with other people using ICT should be polite and friendly and will not deliberately send anything unfriendly or nasty.

Name……..…… Class……
Signature……..

For Parents/Carers

I give permission for my child …… to access the Internet at Forest View Primary School with proper supervision, and to receive and send emails with other children under responsible conditions. I also agree to allow my child's work or images of my child to be displayed as part of the school website, on condition that only a first name is published if necessary. I agree to support the school in education of my child about e-safety.

Signed……

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. Due to recent changes in remote learning and more proficient use of technology in your child's learning, parents should be aware that teachers and other school staff will only respond to contact from children or parents during school hours.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

Parents are requested to sign the permission form below to show their support of our school in this important aspect of Forest View's work.

Use of Cloud Systems Permission Form
Forest View uses Google Drive for pupils and staff. This permission form describes the tools and pupil responsibilities for using these services.

The following services are available to each pupil as part of the school's online presence in Google Drive. Using Google Drive will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer. The school believes that use of the tools significantly adds to your child's educational experience.____

Use of Social Media Sites

As a school, we have decided to share news, events and images via a social media website - Facebook. Parents/Carers are encouraged to visit our school Facebook site to stay informed of upcoming events. Any misuse of our school Facebook page or any inappropriate activity will result in removal of access and legal advice will be sought if deemed necessary.

Pupil Name/s: ……..……..

Parent/ Carer Name/s:……...

Signed:……..……..……
Date:……..

Staff Acceptable Use Policy Agreement

- I have received (have access to a central copy held with all school policy documents) a copy of the school's ESafety/acceptable use policy.
- I will only use the school's e-mail / Internet / Network / Personal e-mail for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only log onto the school Network / Internet using an assigned user account, set up by the school technician by prior request and will not log on with anyone else's individual details. (Group accounts for children should only be used when necessary to set or retrieve work.)
- I will log off from my account when it is not in use to prevent access by unauthorized pupils/staff.
- I will ensure that the pages of my personal social networking sites (facebook/Twitter etc) that I am a member of are of an appropriate nature and that the pages of any 'friends' that I am linked to are also appropriate. Staff have a professional responsibility to ensure personal information is kept private and any references to school are not communicated via social networking sites.
- I will ensure that I will only use Facebook to update the school site. I will not access my personal account at school.
- I will not engage in any on-line activity that may compromise my professional responsibilities. Staff must not agree to become 'friends' with any pupil currently at Forest View Primary School. Should they be asked, they should decline and then discuss the reasons why not with their class in circle time/PSHE.
- I will not allow unauthorized individuals to access Email / Internet / the Network. I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to a member of the e-safety team. I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed. Any downloads should be approved by the school technician.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of antivirus software.
- I will ensure I am aware of digital safe-guarding issues so they are appropriately embedded in my classroom practice.
- I understand that all Internet usage will be logged and this information could be made available to my Head Teacher on request.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.
- Due to recent changes in remote learning and more proficient use of technology in your child's learning, parents should be aware that teachers and other school staff will only respond to contact from children or parents during school hours.

Signed_____

Date _____

Appendix ii)

Reporting an E –Safety Incident – Guidance

Introduction

E-safety incidents can take many forms; from the accidental access of inappropriate content to serious incidents including illegal images or behaviours by adults or children.

The flow diagram is designed as a guidance document to help you ascertain how to respond to an incident, actions you need to take and who to involve. These processes will be reviewed regularly to help ensure you have the appropriate support and information to ensure you act appropriately when incidents arise. We welcome your feedback and encourage you to share this with, in the first instance, Mike Hamilton, who is the LA lead for ICT and based at Open Zone.

Schools do need to be clear in their understanding of the differences between 'inappropriate' and 'illegal' content. Examples of inappropriate content can include soft porn (e.g. 'page three' images), political extremism and online gaming whilst illegal content would include cyberstalking or harassment; internet fraud; dangerous and illegal activities, such as bomb-making, terrorism, or unlicensed trade in weapons; physical threats; hate crimes, such as advocating genocide or violence; copyright violations; hacking: illegally breaking into individual computers or computer networks; child pornography. The school will need to take a view on whether access is deliberate or accidental.

The E-Safety Officer Role

All schools should identify a member of staff to take on the role of e-safety officer. Many schools choose the person who already has a responsibility for child protection, and some identify the headteacher as this can be a very challenging area when serious incidents occur. It is important that whoever is identified has the experience and confidence to respond appropriately when required - and when that person is unavailable, another member of staff can take on this role.

In all instances of an e-safety incident the e safety officer should be notified and log the details in the school's e-safety incident book. By logging even accidental incidents this will help inform filtering policies, AUPs and education and training needs within the school.

Schools should keep a record of the reporting process for each incident to help document that they reported the incident to the appropriate individuals and organisations. The E-Safety Officer should report access to illegal websites via schools systems to the Local Authority E-Safety Contact for Schools.

Adults (including teachers, assistants, governors, visitors etc.)

Where illegal content is accessed deliberately or accidentally the incident needs to be logged, reported to the headteacher and the local authority. Where the incident is believed to be deliberate, the school must also notify the police but must ensure that the Local Authority are informed first.

Although illegal sites are filtered it is unlikely that either a child or an adult will access them accidentally. Having said this, it is a remote possibility that an illegal site displaying child abuse imagery or other illegal images not yet

listed with the Internet Watch Foundation is not filtered and a genuine accidental incident could occur. In some extreme cases the police may need to be informed of accidental access to illegal material; the Local Authority contact will advise schools on the appropriateness of this action when the incident is reported to them. For other illegal content the computer should be isolated and the images etc. not shared with anyone until the correct procedure is followed, reported and recorded.

In either accidental or deliberate cases the equipment will need to be isolated and the local authority or police will arrange for further examination of the device. The local authority will provide assistance in adjusting the in-school filtering and provide further training, support and guidance.

Where inappropriate content is accessed accidentally the filtering policies can be amended and further training and support provided if required. In the case of deliberate access the school should follow established disciplinary procedures, amend filtering and notify the local authority. The local authority will then follow the Northern Grid procedure for reporting.

Children and Young People

The reporting processes remain the same as those for incidents relating to adults. Where illegal activity has taken place accidentally or deliberately, the device needs to be isolated, forensically analysed and restored prior to using again within the establishment.

In the case of either deliberate or accidental access to illegal content it is likely that the person will need counselling and support within school and other agencies. The local authority will be able to assist with identifying this.

Where a child or young person has deliberately or accidentally accessed inappropriate content there is an opportunity to provide further education to the individuals involved and the students. The local authority can provide in-school support and provide information on other sources of information and teaching and learning resources.

In each instance it is important to ensure that parents and carers are aware of the incident and encouraged to support the school's actions.

Illegal Content

Should you encounter something which you suspect to be illegal or suspect that a web site contains illegal material, contact the LA team immediately who will advise and support you. Please do not print out copies of offending information or forward it, or send links to anybody as the transmission of some content is a criminal offence itself.

IF the content is believed to be child abuse imagery they must immediately report it to the IWF as well as notifying the LA. No-one should be informed of the URL as no investigation must be made by anyone other than those licenced to view.

Further assistance is available by contacting Mike Hamilton at Open Zone, South Shields.

Key Contacts

Mike Hamilton (LA E-Safety Contact for Schools) Tel 0191 4272123

mike.hamilton@openzone.org.uk

Beverley Shy (ICT & Information Security Officer) Tel 0191 424 7079

beverley.shy@southtyneside.gov.uk

Appendix iii)

Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority Group or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

Appendix iv)

Using Video Conferencing and Virtual Lessons during School Closures - Covid-19

Due to recent changes in remote learning and more proficient use of technology in your child's learning, parents should be aware that teachers and other school staff will only respond to contact from children or parents during school hours.

Forest View Primary School will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Our school uses Google Suite for Education via our Realsmart platform. This ensures a more secure access to the Google tools and allows the school to personalise access according to need. Specifically:

- Settings have been adjusted so that pupils can only get access to the class Google Meet if the teacher has invited them. Students cannot create a Google Meet.

- This is regardless of whether the teacher sets up a meeting with a code or a calendar invite. The teacher must be in the Meet for pupils to join.

- When finished a teacher needs to leave Meet last otherwise the pupils in Meet can continue. Once Teacher has left no pupils can get back in.

- The only way a pupil can access a Meet if the teacher isn't in is when it is scheduled via a calendar invite, but once the calendar invite is deleted this goes too.

Below are some things to consider when delivering virtual lessons with students, especially where webcams and Google Meet are involved:

1. You should not conduct individual sessions, no 1:1s. Arrange for video conferences with groups only.
2. There should be 2 members of staff in the Meet in order to manage the chat facility and to safeguard all participants.
3. Staff and children must wear suitable clothing, as should anyone else in the household.
4. Any computers used should be in appropriate areas, for example, not in bedrooms; and the background should be blurred or neutral, devoid of personal photographs or items.
5. Live classes should be kept to a reasonable length of time, or the streaming may prevent the family 'getting on' with their day.
6. Language must be professional and appropriate, including any family members in the background.
7. Staff must only use platforms specified by senior managers and approved by our IT network manager / provider to communicate with pupils.
8. Staff should record the length, time, date and attendance of any sessions held.
9. Staff should be aware of any children whose photograph is not allowed to be taken and ensure parents consent to their child's image on screen. If the parent does not want the child to appear live they should turn off the camera using tools in the Meet.

10. All participants should refrain from taking any screenshots, or otherwise taking pictures or recording the session to safeguard and protect the children and staff members taking part.
11. Participants should turn off microphones when taking part unless the teacher asks for them to be turned on.
12. The chat tool should be used to ask the teacher questions and communicate with each other in an appropriate manner.
13. In situations where there cannot be 2 members of staff then the live class should be re-arranged. If this is not possible the live class should be recorded so that if any safeguarding issues were to arise, the video can be reviewed. This recording should be saved in a secure location and deleted as soon as it is not required or within 10 working days.
14. The teacher should set protocols at the beginning of each session to address issues of behaviour and feedback. Reminding students of turning off microphones, cameras and being polite. Any follow up work should be completed and submitted in a timely manner.
15. There may be situations where a session will need to be recorded to aid revision or assessment purposes. This is more likely to be with KS3 and KS4 pupils. Students should be given the option to turn off their camera using the tools.

Recording a virtual teaching session.

Sessions may be recorded for a number of reasons, but in all cases the participants must give their consent to be recorded. If they do not want their image to be displayed they can turn their camera off.

1. Some teachers may want to either stream or produce a webinar style session. In this case it would be necessary to show the presenters screen and to broadcast their voice. An image is not important so all those participating could and should leave cameras off and just have their avatar showing.
2. Teachers may want to produce a video to help explain a concept or read a story. An image is not important so all those participating could and should leave cameras off and just have their avatar showing. The video could be saved and then made available on Google Drive.
3. Should teachers want students to be able to access material to help them after the VC session has ended, they should make a separate resource rather than record the full VC.
4. In some cases recording is necessary because the session might count towards coursework, e.g. a presentation or seminar scenario. Consent should then be collected prior to the session. Students could opt out of their image being shown by using their avatar.

Tips for Teachers

- Make sure you are first into the conference.
- Check the walls behind your head for posters/letters/photographs you might not want to show
- Dress professionally
- Conduct the VC in just as professional way as you would teach a lesson
- Think about how you deal with pupils at risk whose photographs shouldnt be shared
- Have more than one member of staff in the conference so you have somebody to monitor and help facilitate the chat function.
- By using a calendar invite teachers can ask for parental consent for visibility and to abide by the AUP. Suggested text for the invitation:

  By joining this meeting you agree to abide by the AUP and for your child to be visible to others. If you do not wish for your child to be seen, please turn off your camera.

Tips for parents of pupils on VC

- Be in the same room as your son/daughter when they are in the VC
- Think about your own and their attire.
- Reduce distractions - turn off the TV and ensure younger siblings are out of view.
- Do not take pictures of the screen during a VC or video it.

Appendix 1: An exemplar AUP for Virtual Lessons and Video Conferencing - please use and adapt to your school for staff and students.

Some other information around video conferencing and Meet
Your teacher will never

Safeguarding when video streaming

FAQs around recording a Meet
https://support.google.com/meet/answer/9308681?hl=en

Appendix 1

Acceptable Use Policy for Virtual Lessons or Video Conferencing

I agree to:

Only use my school email and account to access a virtual lesson or video conference.

I will be polite and respectful at all times.

I will conduct myself as if I were in the classroom.

I will dress in an appropriate fashion.

I will try to ensure the space where I am working will be suitable.

I will try to minimise distractions.

I will not record any of the sessions or take photographs or screen shots.

Can all staff please add their name and date to the end of this document to say you have read it please?

K. Charlton 29.4.20
S. Archer 29.4.20
A.Rutherford 29.4.20
V.Thompson 29.4.20
K.Waugh 29.4.20
R. Brown 29.4.20
A. Williams 1.5.20

Appendix v)

Safeguarding & Online Safety Policy / AUP Addendum for Home Learning during Covid-19 Closures

During school closures and remote learning, ***the same principles of safeguarding, online safety and behaviour apply – major changes to policy documents should not be needed***. However, schools should review policies, remind stakeholders of existing principles and identify any which need reinforcing due to new (mostly online) procedures and activities.

This document was written with LGfL's template policies in mind (safepolicies.lgfl.net), but is relevant to all schools. Here are some to revisit, remind or reinforce, documents to read and actions to take:

1) The new **DfE Covid Safeguarding Guidance** is essential reading; we have not repeated it here as you should read it in full. Find it as well as this document & our templates at safepolicies.lgfl.net.
2) **Reread then reissue school policies** for online safety, safeguarding and AUPs. First check what needs changing in the light of closure, remote learning and alternative arrangements at school. Use the suggestions below, but don't rely on others to identify issues unique to you.
3) Whatever technology you are using for lessons, **look at the 20 safeguarding principles for remote lessons** in the infographic at coronavirus.lgfl.net/safeguarding (NB no www in the link). The graphic was originally for video and streaming BUT actually applies to all online learning. Examples are not using private accounts, logging all contacts, issues and concerns, considering pupils with SEND, avoiding private chats with pupils, etc. Stick to what you know and can safely operate!
4) There are many **online scams** playing on people's fears and the current situation. See coronavirus.lgfl.net/security for help keeping staff and families safe & secure (including staff training).
5) All policy and AUP issues are worthy of reminders, but especially the importance of critical thinking: not just to combat fake news and scams, but also because of increased **grooming activity relating to radicalisation or child sexual exploitation** as a result of greater online access to children.
6) Whatever Key Stage you teach (even secondary!) look at our KS1 AUP because the simple language used for **11 top tips to stay safe online** are the essentials of online safety (safepolicies.lgfl.net).
7) Remind those with access to school devices about rules on the **misuse of school technology** – devices used at home should be used just like if they were in full view of a teacher or colleague.
8) How are you **helping parents to keep children safe**? The Top Tips poster at the link above is a starter; for more resources, share relevant items from parentsafe.lgfl.net (not the whole collection).
9) In school you have 'appropriate filtering' but at home many parents will not be using **parental controls**, so remind them to do so (Internet Matters has guides). Now is also a good time to introduce **child-safe search engines** e.g. swiggle.org.uk and **YouTube Kids** instead of YouTube.
10) Lots of people are offering their services on social media to give **online tuition to other people's children**. Remind parents not to engage someone they do not know, that they should listen in where possible, any sessions should be in family areas not bedrooms, and that children need to be told that tutors should not arrange new sessions or online chats directly with them.
11) Do you have **new volunteers** working with children in school or at home or remotely? Do they know your safeguarding rules? Are they DBS checked? Are precautions in place?
12) Are any **staff working one-to-one** with pupils in new ways or in parts of school which are emptier than usual? How is this logged and monitored? Keep children and staff safe by planning for this.
13) Have your **reporting functions** changed? Can pupils and staff flag issues when not in school? Do you need alternatives? Who is monitoring them (if all your DSL team get sick, would somebody pick up the messages)? Do you need a new channel (e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox)?

14) Can you send a **safeguarding bullet point reminder to staff each day** in the same way as you may have previously done at the start of face-to-face briefing?
15) **Staff training** will not be happening face to face, so make the most of online CPD opportunities, especially after Easter once a routine is settled. See safecpd.lgfl.net for ideas. NB: the DfE guidance above states that DSLs missing refresher training can continue to operate as a DSL.
16) Do you need to **communicate your policies** (including any changes and reminders prompted by the above) in new ways during closure? Are the online versions current / sufficient / available to all (do all links still work / have you changed systems)?

SEE OVER FOR TEMPLATE FORMS TO ADAPT AND USE IF THEY ARE USEFUL

1) This record will be far more effective if you paste the questions into your school-linked online account of choice, e.g. Microsoft or Google Forms, rather than email out as an attachment (we have not done so as it needs to be linked to your account).
2) Tell staff which systems are pre-authorised and which ones they do not need to tell you about (e.g. if the whole school is using Google Classroom to issue and collect all work, then you may ask them to only notify you of unusual activity or concerns. Alternatively, you may only need a form for those contacting or visiting vulnerable children.
3) Remember to share this with new staff or volunteers and ask for more logging from them.

Staff or volunteer name	Other staff present (if a live video, stream or chat)	Name of class, group or individual	Time and frequency (e.g. weekly on Tuesday at 10am or specific date)	Scheduled? (Y / N)	Platform used. Only use school accounts!	Issues, worries, concerns (technical, safeguarding, DP or other) and general trends. ** If a one-to-one conversation, where is the summary? **