Woodford Valley C of E Primary Academy
Online Safety Policy

Signed……

Date …..September 2024

Review…September 2025

This school is committed to creating the ethos in which children can grow towards Christian life, learning and love.

And now I give you a new commandment: love one another. As I have loved you, so you must love one another. If you have love for one another, then everyone will know that you are my disciples."
John 13 34-35

This policy is intended to be read in conjunction with all other policies and in particular the Child Protection Policy, Anti-bullying Policy, Online learning protocol, Responsible internet use agreement and Photographic Policy.
This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Intent

At Woodford Valley C of E (VA) Primary Academy we embrace new technologies using a wide range in school as valuable tools to enhance both learning and teaching, and to explore and enjoy the world we live in. Pupils at our school have easy access to a variety of ICT resources that aid and develop their knowledge and understanding of all curricular and cross-curricular areas. They use these resources to organize their learning and communicate with their peers, teachers, parents and the outside world.
Likewise, adults that work within our school community use these resources to:

- further their professional development
- to search for enriching and supportive materials
- to strengthen the links with parents and outside agencies
- to coordinate the assessment and progress of individuals and groups of learners
- to ensure that both excellence and enjoyment drive the vision of ICT within our school community

Our school Internet Safety Policy will feature as part of the review process within the School Development Plan. It should relate to other policies including those for behaviour, for personal, social and health education (PSHE), for bullying and for citizenship.

- Our Internet Safety Policy has been written by the school, building on the SWGFL online-safety template policy and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually. Scope of the Online Safety Policy
- This Online Safety Policy outlines the commitment of Woodford Valley Primary Academy to safeguard members of our school community online in accordance with statutory guidance and best practice. Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.
- This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).
- Woodford Valley Primary Academy 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.

Leadership and Management

Responsibilities
To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

- The Head Teacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Head Teacher 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[2].
- The Head Teacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Head Teacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Head Teacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.

[1] In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.
[2] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

- The Head Teacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"
"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
This review will be carried out by the (insert name of governor group/committee) whose members will receive regular information about online safety incidents and monitoring reports. A member of the governing body will take on the role of Online Safety Governor to include:

• regular meetings with the Designated Safeguarding Lead / Online Safety Lead
• regularly receiving (collated and anonymised) reports of online safety incidents
• checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
• Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards
• reporting to relevant governors group/meeting
• Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards
• membership of the school Online Safety Group

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

Designated Safety Lead (DSL)

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description." They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

They (the DSL) *"*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"
While the responsibility for online safety is held by the DSL and cannot be delegated, the school may choose to appoint an Online Safety Lead or other relevant persons to work in support of the DSL in carrying out these responsibilities. It is recommended that the school reviews the sections below for the DSL and OSL and allocate roles depending on the structure it has chosen

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
- attend relevant governing body meetings/groups
- report regularly to Head Teacher/senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Lead

The Online Safety Lead will:

• lead the Online Safety Group
• work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), (where these roles are not combined)
• receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments
• have a leading role in establishing and reviewing the school online safety policies/documents
• promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
• liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
• ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
• provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
• liaise with (school/local authority/MAT/external provider) technical staff, pastoral staff and support staff (as relevant)
• receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:

- content
- contact
- conduct
- commerce

Curriculum Leads

Curriculum Leads will work with the DSL to develop a planned and coordinated online safety education programme
This will be provided through:

- PHSE and SRE programmes
- Assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- Teaching and support staff

Authorised Internet Access

Internet access for pupils should be seen as an entitlement on the basis of educational need and an essential resource for staff. Parental permission is sought at the start of each child's learning journey.

The school Internet Service Provider (ISP) is Oakford Internet Services. Monitoring reports will be produced by the ISP on regular request.

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn.
- Primary pupils' home-school agreement will include the Responsible Use Policy agreement.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved online materials wherever possible.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Pupils will be given a personal Microsoft Teams log in and a personal password for use as a remote learning platform. Pupils will be supervised on Teams in school and it is expected that Parents supervise their children using this at home.

Managing Filtering

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider (Oakford) and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access must be appropriate for all members of the school community from youngest pupil to staff and volunteers.

- A log of all access to the Internet will be kept and regularly reviewed.
- The school will work in partnership with parents; Wiltshire Council, DFE and its ISP to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the ISP via the internet safety lead.
- Website logs will be regularly sampled and monitored.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).
- Monitoring systems are implemented and regularly updated as agreed in school policies

Risk Assessment

As the quantity and breadth of the information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

- In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the ISP is implemented and compliance with the policy monitored.

Implementation

The Curriculum

The internet is an essential resource to support teaching and learning. The statutory curriculum requires pupils to be responsible, competent and creative users of information and communication technology, and in doing so, learn how to locate, retrieve and exchange information using technology. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed ICT is viewed to be an essential life-skill.

- internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The purpose of internet use in school is to raise educational standards, to promote pupil achievement, ensure wellbeing and to support the professional work of staff and to enhance the school's management information and business administration systems.

- internet access is an entitlement for students who show a responsible and mature approach to its use.
- The internet is an essential part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
- Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.
- With the possibility of partial closure and/or future lockdowns the internet will play an increasingly important role in continuing teaching and learning remotely.

Enhancing Teaching and Learning using the internet

Benefits of using the internet in education include:

- Access to worldwide educational resources;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments;
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient, including at home if shielding or isolating or during partial or whole school closure.

Evaluating internet Content

Information received via the web, email or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.

Ideally inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the ISP and Wiltshire council.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Communication and Content

Website and class teams content

School websites provide a valuable platform for communicating with pupils, parents and the wider community and inspire pupils to publish work of a high standard. Publication of any information online should always be considered from a personal and school security viewpoint. Sensitive information is better published in the school handbook or on a secure online area which requires authentication. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

- The point of contact on the school website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs will be selected carefully in line with parental permission.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- The nature of all items uploaded will not include content that allows the pupils to be identified.
- The Head Teacher and governors will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.
- Parental permission will be asked for pupils to share their work with their class Team on Microsoft Teams.

Managing email

Email is an essential means of communication for both staff. However, the use of e-mail requires appropriate safety measures.

- Staff will use official school provided email accounts.
- Email sent to an external organisation should be written carefully and on occasions, will be authorised before sending, in the same way as a letter written on school headed paper.

On-line Communications, Social networking and Social Media

On-line communications, social networking and social media services are filtered in school by the ISP, but are likely to be accessible from home.

All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. School takes a key role in teaching young people about the importance of keeping personal information safe.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, site usernames and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, including the tagging of photos or videos, or arrange to meet anyone.
- Staff official blogs or wikis should be password protected and run with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- No member of the school community should publish specific and detailed private thoughts about the school and its practices, especially those that may be considered threatening, hurtful or defamatory.
- Parents wishing to photograph or video at an event are made aware of the school's expectations and be required to comply with the school's policies.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school's Responsible Use Policy.
- It will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Mobile phones and personal devices

Mobile devices refer to any device that provides access to the internet or internal network, for example, tablets (Apple, Android, Windows, and any other operating systems), e-readers, mobile phones, iPad, iPod Touch, digital cameras/video.

Mobile devices can be used to facilitate communication in a variety of ways with text, images, sound and internet access all being common features. Staff should be given clear boundaries on professional use of personal devices in school.

- Mobile devices that are brought into school remain the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items.
- Staff are expected to use mobile phones responsibly, in line with the staff Acceptable Use agreement.
- School staff authorised by the Head Teacher may search pupils and their possessions, and confiscate any mobile device they believe is brought into school by pupils and used to contravene school policy, constitute a prohibited item, is considered harmful, or detrimental to school discipline. If it is suspected that the material contained on a mobile device relates to a criminal offence, the device will be handed to the Police for investigation.

- KS2 pupils have been authorised to bring to school their own personal laptops for use in school, providing the pupil and parents have agreed and signed the laptop policy
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community.
- Mobile devices will not be permitted to be held or used in school by pupils.
- Mobile devices are not permitted to be used in certain areas within the school site such as changing rooms or toilets, situations of emotional distress.
- Where staff may need to contact children and their families within or outside of the school setting in a professional capacity, they should only do so via an approved school account, such as e-mail, phone, learning platform). In exceptional circumstances, there may be a need to use their own personal devices or account; this should be notified to a senior member of staff immediately.
- Staff should be provided with school equipment for the taking of photos or video of pupils linked to an educational purpose and intention. They must not use personal devices such as mobile phones or cameras to take photos or videos of pupils. In exceptional circumstances, staff may need to use personal devices for such a purpose, however and when doing so, should comply with the school's Acceptable Use Policy and notify a senior member of staff.
- For the safeguarding of all involved, users are encouraged to connect mobile devices through the school's wireless guest Wi-Fi provision and service that allows the ability to filter any device that uses the school Internet connection, without having to configure the user's device.
- The school will take steps to monitor responsible use in accordance with the Acceptable Use Policy.

Video Conferencing

Video conferencing, (including Microsoft Teams, FaceTime, Zoom Skype and Lync) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education and where possible, should take place using the school's wireless system.

- Staff must refer to any Responsible Use agreements prior to children taking part in video conferences.
- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Pupils will ask permission from a teacher before making or answering a video conference call.
- Video conferencing will be supervised appropriately for the pupils' age and ability.
- Where possible staff will undertake live lessons in school. However there may be times such as bubble isolation where this is not possible. In this case any video conferencing will take place with a neutral background.
- Parents are expected to supervise their children when using Microsoft Teams for remote learning at home and for younger children parents are expected to be on hand during online lessons to support their children.
- As outlined in the Online learning protocol parents and pupils will agree to not record or photograph any part of an online lesson. Access will be withdrawn with immediate effect if this happens.
- Parents are requested to remove their child's mobile during live lessons.
- Joining a meeting with video is completely optional. There will be no expectation from the school for students to join with video. Parents and pupils are reminded that privacy in family homes is of great importance and that they remain fully in control of what they choose to share.
- When taking part in a video call from home, pupils must be in a shared family space and be appropriately dressed.

- Pupils are requested to join meetings larger than individual classes with both their camera and microphone turned off.
- Parents are reminded that the on-line lessons are for those children who are not attending in school, any parent/carer whose child is in school that joins the on-line lesson will be removed from the session immediately.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom and school-wide use. Our approach is to deny access until a risk assessment has been completed and safety has been established.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use for learning remotely or in school is allowed.

The use of online learning platforms has rapidly evolved since the coronavirus pandemic emerged and will continue to do so. The school recognises that current policies and protocols will not cover every eventuality. The school will continue to monitor the use of different platforms for online learning and evolve best practice and protocols as they develop.

Cyber bullying

Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” DCSF 2007.

For most, using the internet and mobile devices is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It is essential that young people, school staff and parents and carers understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school’s policy on anti-bullying and behaviour.

- Clear procedures are in place to investigate incidents or allegations of cyber bullying. within school
- Clear procedures are in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying on all school systems reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the Internet Service Provider and the police, if necessary.
- Curriculum content will ensure that pupils and parents are informed and educated about cyber bullying, including cross-curricular activities, assemblies, information workshops.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyber bullying and the school’s e-safety ethos.

Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The GDPR Policy gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Implementation

Policy in Practice: Pupils

Many pupils are very familiar with Internet use and the culture that surrounds it. As part of the school's e-safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age and development. Pupils may need to be reminded of the school rules at the point of Internet use.

- All users will be informed that network, internet and email use will be monitored.
- All users are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)
- Online safety teaching is integrated into the curriculum to raise and develop awareness about the importance of safe and responsible internet use amongst pupils.
- Online safety teaching will be included in the PSHE, Citizenship and Computing programmes and will cover safe use of the Internet at both school and home.
- E-safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with internet access and on class webpages
- Safe and responsible use of the internet and technology will be reinforced across the curriculum and subject areas.
- All pupils are expected to use Microsoft Teams responsibly. The school will check Teams files, chat and profiles. In the event that these rules above are not followed or any inappropriate use parents/carers will be contacted. If issues persist, access to Microsoft Teams will be removed.
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Policy in Practice:

Staff School staff are responsible for ensuring that:

• they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
• they understand that online safety is a core part of safeguarding
• they have read, understood, and signed the staff acceptable use agreement (AUA)
• they immediately report any suspected misuse or problem to (insert relevant person) for investigation/action, in line with the school safeguarding procedures
• all digital communications with learners and parents/carers are 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
• ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
• they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
• in lessons where internet use is pre-planned learners are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
• where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies (n.b. the guidance contained in the SWGfL Safe Remote Learning Resource
• there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
• they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Policy in Practice: Parents

Parents need to be aware of the potential dangers that are associated with online communications, gaming, online gambling, inappropriate advertising, phishing, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk. The school can refer parents to websites providing relevant support and information.

- Parents' attention will be drawn to the school internet Safety Policy in newsletters, the school brochure/prospectus and on the school website.
- Parents are made aware of the Responsible Internet use agreement and Online learning protocol.
- Parents are responsible for supervising their children when using Microsoft Teams for remote learning at home.
- A partnership approach with parents is encouraged. This shall include offering parent evenings, demonstrations, practical sessions and suggestions for safe internet use at home.
- Parents are made aware of the GDPR Privacy Notice.
- Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and at home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet will be made available to parents.
- All parents will receive support information as and when available. Parents and carers will be encouraged to support the school in:
- Parents will be encouraged to reinforce the online safety messages provided to learners in school.
- Parents will be encouraged to support the school in the safe and responsible use of their children's personal devices in the school (where this is allowed)

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations. All members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in the appendix), the incident must be escalated through the agreed school safeguarding procedures, this may include

  - Non-consensual images
  - Self-generated images
  - Terrorism/extremism
  - Hate crime/ Abuse
  - Fraud and extortion
  - Harassment/stalking
  - Child Sexual Abuse Material (CSAM)
  - Child Sexual Exploitation Grooming
  - Extreme Pornography
  - Sale of illegal materials/substances
  - Cyber or hacking offences under the Computer Misuse Act
  - Copyright theft or piracy

- any concern about staff misuse will be reported to the Head Teacher, unless the concern involves the Head Teacher, in which case the complaint is referred to the Chair of Governors and the local authority / MAT
- where there is no suspected illegal activity, devices may be checked using the following procedures:
  - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
  - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
  - ensure that the relevant staff 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

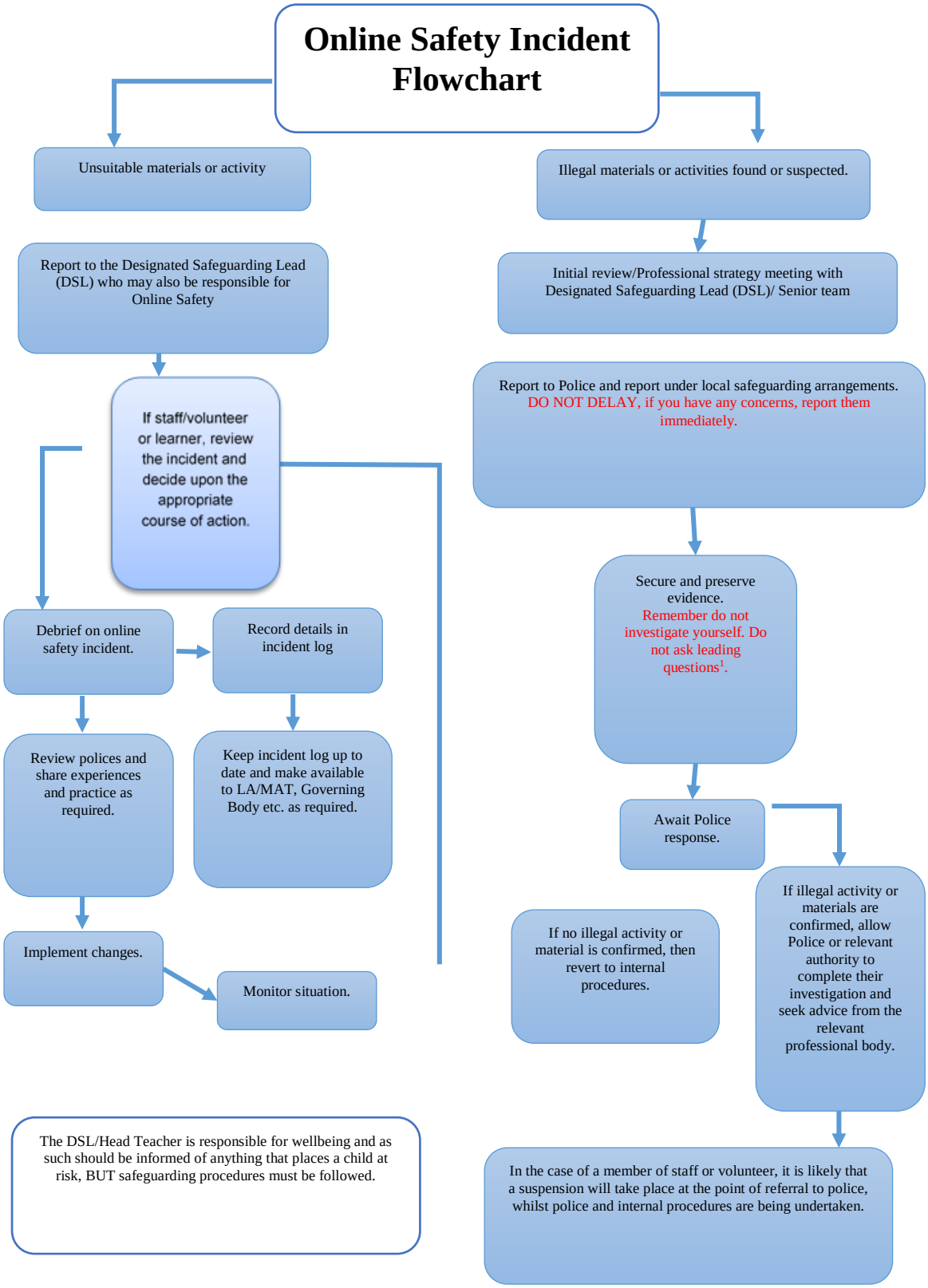
- once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - internal response or discipline procedures
  - involvement by local authority / MAT (as relevant)
  - police involvement and/or action

- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g. peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here). (A template reporting log can be found in the appendix, but many schools will use logs that are included with their management information systems (MIS).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

  - staff, through regular briefings
  - learners, through assemblies/lessons
  - parents/carers, through newsletters, school social media, website
  - governors, through regular safeguarding updates
  - local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour"

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents -

Online Safety Incident Flowchart



Handling of Complaints

Parents and teachers must know how and where to report incidents. Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. All record of the incident should be kept, e.g. emails saved or printed, text messages saved, and so on. Complaints of a child protection nature must be dealt with in accordance with the LA Child Protection procedures.

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact should be made to establish the legal position and discuss strategies.