Western Downland C of E (VA) Primary School

Online Safety Policy

Name of School:	**Western Downland C of E (VA) Primary School**
Name of Responsible Manager/Headteacher:	**Alice Tubbs Headteacher**
Date Policy approved and adopted:	**September 2025**
Date Due for review:	**September 2026**

Statement of Intent

Children interact with the internet and other communication technologies such as mobile phones on a regular basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction is greatly beneficial but can occasionally place young people in danger.

This policy aims to ensure there is the right balance between controlling access to technology, setting rules and educating children for responsible use. Online safety comprises all aspects relating to children and their safe use of the internet and other technologies. This Online Safety Policy outlines the commitment of Western Downland CE VA Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The 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).

Western Downland CE VA Primary 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.

This Online Safety Policy has been developed by the school and will be reviewed annually by staff and Governors. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor.

The policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- describes how the school will help prepare learners to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms

- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and through normal communication channels (staff meetings, emails and notice boards)
- is published on the school website.

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 and groups within the school.

Headteacher and senior leaders

- The headteacher 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 may be delegated to the Online Safety Lead.
- 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.
- The headteacher/senior leaders are responsible for ensuring that all staff follow policies, processes and procedures and act on reports and concerns.
- The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff understand and carry out their responsibilities effectively, receiving suitable training to enable them to carry out their roles.
- The headteacher/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 and review the effectiveness of the schools provision.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

- The headteacher/senior leaders will work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

- The headteacher/senior leaders are responsible for procuring filtering and monitoring systems and documenting decisions on what is blocked or allowed and why.

Governors

The Governing body has overall strategic responsibility for filtering and monitoring and needs assurance that the standards are being met. Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

This review will be carried out by the Full Governing Body 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 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)
- reporting to the FGB
- identifying and assigning the roles and responsibilities of staff and

external service providers

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

Online Safety Lead

The Online Safety Lead will:

- work closely on a day-to-day basis with the Designated Or Deputy Designated Safeguarding Lead (DSL/DDSL)
- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- 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
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with technical staff, pastoral staff and support staff (as relevant)
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings
- report regularly to the headteacher/senior leadership team.
- liaises with the local authority

Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

The DSL should work closely together with IT service providers to meet the needs of the school. The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

Curriculum Leads
Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme.

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

Teaching and support 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 the DSL or DDSL for investigation/action, in line with the school safeguarding procedures
- take steps to maintain awareness of how devices are being used by pupils
- Staff will report if they witness or suspect unsuitable material has been accessed; they can access unsuitable material ; they are teaching topics which could create unusual activity on the filtering logs ; there is failure in the software or abuse of the system; there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks ; they notice abbreviations or misspellings that allow access to restricted material
- all digital communications with learners and 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
- 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 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

- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource
- have 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.

Network manager/technical staff (Trailblaze)

The network manager should work with the Headteacher/senior leaders & DSL to procure systems, identify risk & carry out reviews.

The network manager is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- monitoring software/systems are implemented and regularly updated as agreed in school policies
- they maintain filtering and monitoring systems and ensure they are working as expected
- they provide filtering and monitoring reports on pupil device activity ensuring that data is received in a format that staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL
- they complete actions following concerns or checks to systems

Learners

- 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.

Parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- publish information about appropriate use of social media
- seeking their permissions concerning digital images, cloud services etc.
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school

Community users

Community users who access school systems/website/learning platforms as part of the wider school provision will be expected to sign a **Community User Acceptable Use Agreement** before being provided with access to school systems.

Online Safety Group

The Online Safety Group has the following members:

- Online Safety Lead
- Designated/ Deputy Designated Safeguarding Lead
- online safety governor
- online safety ambassadors

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school Online Safety Policy/documents
- the production/review/monitoring of the school filtering policy (if possible and if the school chooses to have one) and requests for filtering changes
- mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
- reviewing network/filtering/monitoring/incident logs, where possible
- encouraging the contribution of learners to staff awareness, emerging trends and the school online safety provision
- consulting stakeholders – including staff/parents/carers about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users. We recognise 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 policies.
- 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, the incident must be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- 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.
    - 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
        - 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 on CPOMS.
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided to:
    - the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the

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

School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Online Safety Education Programme

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 for all year groups
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- The programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- learners should be encouraged to adopt safe and responsible use both within and outside school
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners 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

- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of 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
- The online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
- the Online Safety Lead and Designated Safeguarding Lead (or other

nominated person) will receive regular updates through attendance at Local Authority network events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- The Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority
- participation in school training / information sessions for staff or parents

A higher level of training will be made available to (at least) the Online Safety Governor.

Families

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.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc
- the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.
- letters, newsletters, website, learning platform,
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant websites/publications
- Sharing good practice with other schools in clusters and or the local authority.

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- the school will provide online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision

Technology

The school is 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. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering

- A review of filtering and monitoring will be carried out annually (or when a safeguarding risk is identified ; there is a change in working practice; new technology is introduced) to identify current provision, any gaps, and the specific needs of your pupils and staff.
- Filtering systems will be age and ability appropriate for the users, and be suitable for educational settings
- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours
- The filtering provided meets the standards defined in the UK Safer Internet Centre & KCSIE 2023.
- access to online content and services is managed for all users including guests, on all school owned devices and devices using the school broadband connection.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- Requests for filtering changes should be sent to the school's network

provider following approval by the Headteacher
- younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

- signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) and block access to illegal content including child sexual abuse material (CSAM)

- handle multilingual web content, images, common misspellings and abbreviations

- identify technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them

- provide alerts when any web content has been blocked

- Filtering will allow the identification of device and individual name, time and date of attempted access and the search term or content being blocked

If necessary, the school will seek advice from, and report issues to, the network provider.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- An appropriate monitoring strategy for all users has been agreed and users are aware that the network is monitored. The online safety lead is responsible for managing the monitoring strategy and processes.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice
- Technical monitoring systems are up to date and managed and alerts are regularly reviewed and acted upon.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)

- internet use is logged, regularly monitored and reviewed
- The school's network manager regularly monitor and record the activity of users on the school technical systems

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Online Safety Group
- all adults have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone.
- the master account passwords for the school systems are kept in a secure place
- passwords should be long.
- The school's network provider are responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- Users should report any actual or potential technical incident/security breach to the school's network provider.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 endpoint (anti-virus) software.
- The provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems is in place.
- School devices may not be used for personal use out of school.
- Requests to download executable files and install programmes on school devices should be sent to the school's network provider following approval by the Headteacher.
- Portable media may not be used on school devices without specific permission.
- systems are in place that prevent the unauthorised sharing of

personal data unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, 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 which may include the school learning platform and other cloud-based services such as e-mail and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to those for safeguarding, behaviour, anti-bullying, acceptable use, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

Mobile Phones

Staff Personal Mobile Phones

- Staff must not carry personal mobile phones while working. This protects staff from being distracted from their work and from allegations of inappropriate use.
- Phones must be safely stored in a locked cupboard. If staff have a break time during their working hours, they may use their mobile phones during these times in the staff room or an office where children are not present.
- In an emergency, staff needing to make a personal call during a lesson or whilst on duty should first obtain agreement from their line manager, ensure that adequate cover has been put in place and make the call in an area not used by children.
- Staff must give the site telephone number to their next of kin in case it is necessary for the staff member to be contacted, in an emergency, during working hours.
- A personal mobile phone may be taken on school trips in accordance with guidance – see 'The Use of Mobile Phones on Trips' section below.
- Camera or video functions on personal mobile phones must not be used by staff to take images of children under any circumstances.
- Staff are not required to make work calls on their own phones, either mobile or landline, however, in exceptional circumstances, if this

should be necessary then they are advised to use the prefix 141 before dialling the recipient’s number to ensure their own number is protected.
- Staff must never store parents’, carers’ or children’s telephone numbers on their mobile phones and staff must never give their private mobile number to parents, carers or children.
- Failure by staff to comply with the mobile phone policy guidelines could result in disciplinary action.

Children

- Children who walk to and from school without an accompanying adult may carry a mobile phone for safety. In these cases, children may bring a mobile phone on to the site but must deposit it with the school office at the start of the day and collect it from the office at the end of the day.
- Parents and carers need to be aware that whilst there are obvious benefits to pupils having a mobile phone in terms of personal safety there are also some associated risks such as potential for theft, bullying and inappropriate contact, including grooming by unsuitable persons.
- We would also like to alert parents and carers to the risks that using a mobile phone has while walking to and from school. Children who are concentrating on using their phone can have reduced general safety awareness which may result in road accidents and/or injury if a child is not paying attention to their surroundings.
- Mobile phones deposited in the office by children will be kept safely in a locked cupboard. Whilst the school will take every reasonable care, it accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile phones. It is the responsibility of parents and carers to ensure mobile phones are properly insured. It is recommended that pupil’s phones are security marked and password protected.
- Children are not allowed to bring mobile phones into any other areas of the school. Any mobile phones discovered to have been brought into the school and not handed in to the office will be confiscated immediately. Parents or carers will be asked to collect the mobile phone from the school office.
- Children are not allowed to carry mobile phones on any school trips.
- If a member of the staff has any suspicion that a mobile phone brought into school by a pupil has unsuitable material stored on it, the pupil will be required to hand over the phone immediately to a member of staff and parents or carers will be asked to collect it from a member of the senior leadership team. In circumstances where there is a suspicion that the material on the mobile phone may provide evidence relating to a criminal offence the phone will be handed over to the school’s safeguarding lead or to the head teacher for further investigation and the parent or carer asked to collect it

from them.

Visitors, Parents and Carers

- We ask all parents not to use mobile phones in school from 9am until 3.30pm. This includes all uses including, texting and photographing.
- Visitors and supply staff are not allowed to use mobile phones on the school site and phones must be kept in their bags.
- Mobile phones can be used in the staff room.
- If a visitor, parent or carer is seen using their mobile phone, they will be asked politely to turn it off/desist from using it/remove it from children's view.
- It is recognised that many parents and carers use their mobile phone as a camera/video device to record their child at special performances e.g. school worship, concerts, etc. On these occasions the use of a phone is permitted for photographing/videoing only; images should only be taken by parents and carers if they include their own child and that the use of these images is for their own personal use and must not be uploaded for any internet use including Facebook or any other social networking sites or used in any form of publication unless they are solely of their own child.
- The school recognises that children may inadvertently be included in photographs by another parent; the school, therefore, are obliged to warn parents and carers of the legal and safeguarding risks of publishing such photographs on any platform. The placing of any photographs of children on social media is dangerous and parents may be in breach of the Data Protection Act if they upload photos of other children without the explicit consent of that child's parents.

Use of Mobile Phones on School Trips

Carrying mobile phones on trips can help to ensure safety for all members of the school. However, it is important that the following guidance is adhered to in order to keep children safe and protect staff and volunteers from accusations of inappropriate use:

- Personal phones should only be used to contact staff members or volunteers on the trip, the school or emergency services. If possible, these calls should be made away from children.
- Personal phones should not be used for any purpose other than school business for the duration of a trip. This means that personal calls or texts should not be made or accepted. On residential trips this will apply while the member of staff or volunteer is on duty.
- Staff and volunteers should ensure that next of kin are provided with the site number so that in an emergency the site is contacted and will make contact with the relevant person through the leader. If it becomes necessary for a member of staff or volunteer to make a personal call or text, then the leader or another member of staff should be informed and take responsibility for the pupils in the group while the call or text is made away from sight and sound of

any pupils.

- Personal mobile phones must not be used under any circumstances to take photographs or videos of pupils.
- Volunteers are acting role models for the duration of the trip and therefore must not take photos or videos of any pupils, including their own child, using a mobile phone or any other mobile device, e.g. camera or tablet, without the express permission of the leader.
- Volunteers may be asked to take photographs of their group using a school or centre device – this must be passed back to the leader at the end of the trip.
- The leader may ask volunteers to provide them with their mobile phone number for the duration of the trip so that they can be contacted in case of emergency. The leader undertakes to ensure that these numbers are not held on any mobile device or in any written form after the end of the trip. It is advised that if the leader is using his or her own mobile phone, then if they need to contact anyone during the trip they do so by pre-dialling 141 (some mobile providers use a different prefix – staff are advised to check this with their provider) before the number so that their own number remains protected

Social media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues
- clear reporting guidance, including responsibilities, procedures and sanctions
- risk assessment, including legal risk
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- a process for approval by senior leaders

- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- personal communications which do not refer to or impact upon the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school should effectively respond to social media comments made by others according to a defined policy or process
- 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.

School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and learners need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying 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. It is common for employers to carry out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes
- 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 is 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 learners in the digital/video images
- staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- images will be securely stored in line with the school retention policy

- learners' work can only be published with the permission of the learner and parents/carers.

Communication

When using communication technologies, the school considers the following as good practice: When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users must immediately report, to the Headteacher, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school email addresses should be used to identify members of staff and learners.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through (amend as necessary):

- Public-facing website
- Social media
- Online newsletters

The school website is managed/hosted by All Solutions. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where learners work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- has a Data Protection Policy.
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.
- has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
- has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
- The information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
- will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
- data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals

- provides staff, parents and volunteers with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
- has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
- understands how to share data lawfully and safely with other relevant data controllers.
- has clear and understood policies and routines for the deletion and disposal of data
- reports any relevant breaches to the Information Commissioner within 72 hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- has a Freedom of Information Policy which sets out how it will deal with FOI requests
- provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

- data will be encrypted, and password protected.
- device will be password protected.
- device will be protected by up-to-date endpoint (anti-virus) software
- data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
- only use encrypted data storage for personal data
- will not transfer any school personal data to personal devices. Procedures should be in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).
- use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end

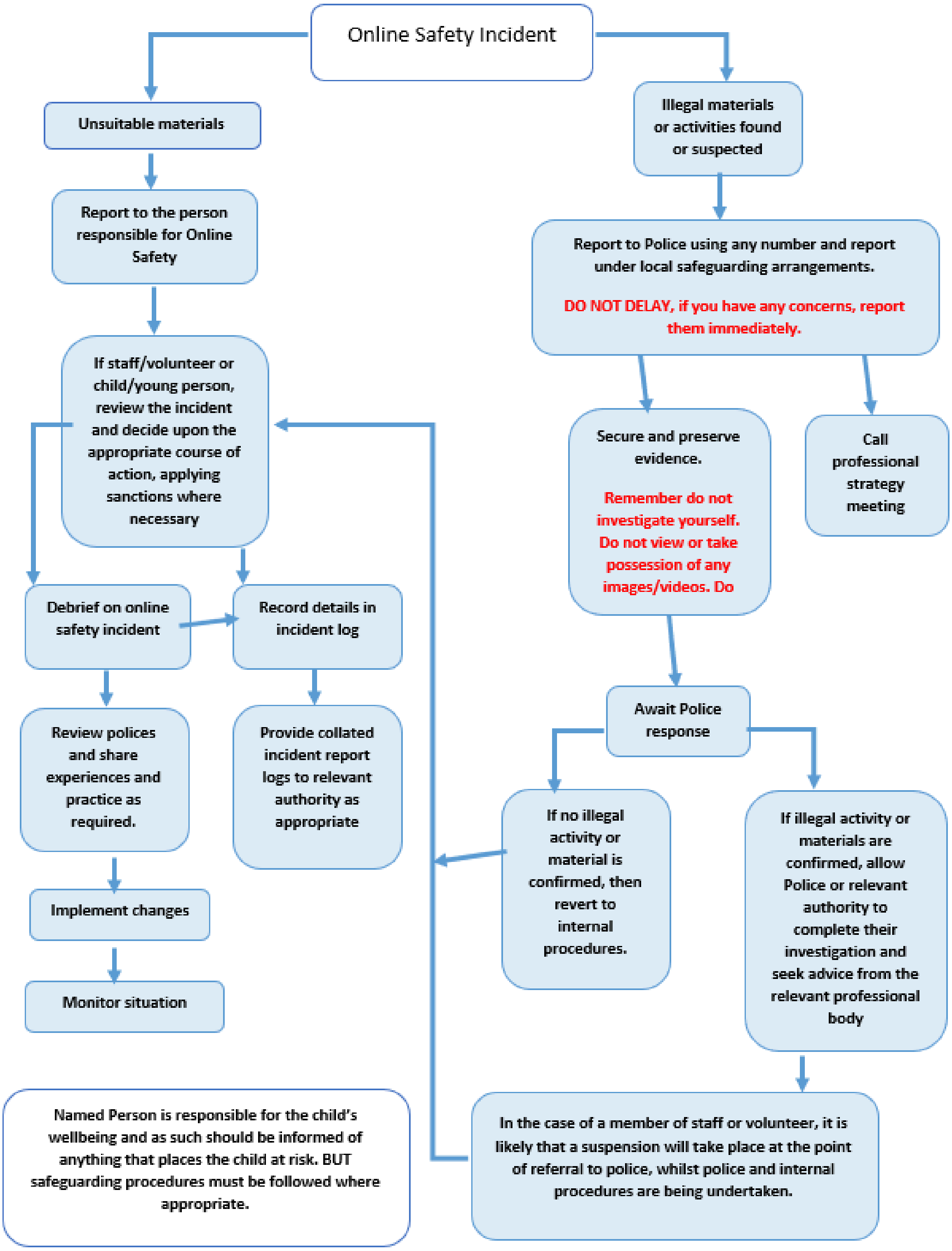
of any session in which they are using personal data
- transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website
- Home/school agreement
- peer support

Responding to incidents of misuse – flow chart



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.