Grove Vale Primary School

Acceptable Use Policy

Date: November 2026

Review: November 2029

A.Cotterill

Mission Statement linking to Computing

At Grove Vale, we strive to provide a welcoming, nurturing and caring environment where our pupils can flourish and exceed their potential in all aspects of their development, our motto devised by a pupil is Together We Grow. We encourage pupils to use our core values, which underpin our school ethos and teaching and learning. Our values aim to expand our pupils' minds, developing confident, resilient and articulate learners ready for life in the diverse and technological world we live in. We aim to provide a foundation for our pupils to value each other and our community, respecting the rights of each other in both the real world and the digital. We ensure that our welcoming, secure and visually stimulating environment supports our staff and pupils to promote a love of learning every day. We grow together with grace, valour, pride, success empowering our ambitious pupils to strive to be the very best they can be in partnership with parents, governors and the community, leaving a positive footprint virtually and physically.

Introduction and Policy Aims

The use of information and communication technology is an integral part of the National Curriculum and is a key skill for everyday life. Our curriculum allows our children to have frequent opportunities to use and apply skills that involve technology. Computers, Chrome Books and Ipads are just a few of the devices that we use in school. The curriculum allows deep links with a range of subjects (maths, science, English, art and music to name a few), which offer opportunities to further develop and consolidate knowledge of computing and online safety, understanding and skills in these areas. To ensure children are able to reap the benefits of using technology to enhance their learning children and staff must be aware of potential risks and be able to effectively make choices in reference to technology and behaviour online in order to safeguard themselves. This continues to become increasingly more important as the use of technology within school for both staff and pupils is continually growing.

The purpose of this policy is to state how the school provides guidelines for both children and staff in order to provide safeguard and protect them by outlining school's expectations. It is to function alongside the online safety policy, computing policy and other policies that link directly to information regarding reporting, use of technology, use of the internet, etc. It is to build awareness amongst staff, pupils and visitors of acceptable use of technology in reference to school and to consider these guidelines to further support them in their own personal use of technology at home and in the future. It is to consider the risks and dangers that could potentially happen and prepare them with knowledge that will prevent and support them when using devices and accessing the wide range of online elements that we use both in and out of school.

It's purpose is also to ensure that staff follow GDPR guidelines. In addition to this, it aims to support children to be safe, positive and successful digital citizens through the teaching and learning of online safety, which is embedded regularly throughout our school curriculum and the opportunities

we provide for our children. The benefits of the online world and use of technology for both staff and pupils exceed the disadvantages. The responsibility to ensure safeguarding online is met is one of the collective, including governors, parents and carers.

Use of Technology

All users within school (including staff and children) are encouraged to use facilities provided in reference to educational purposes. All users must take full responsibility for the way they use technology and the device they use or own. Technology, including mobile phones, tablets, MP3 players, memory cards, cameras, IPads, Chrome Books, Laptops, etc, should all be used responsibly in relation to guidance provided within the policy and additional policies that link to AUP such as the mobile phone policy. All users must make sure that they use technology safely, responsibly and legally. They should also take part in online safety training, which consolidates expectations of this, and actively participate in building an effective online safety education, which is ever evolving and changing.

Network Security

All users of the network, including staff and pupils, are provided with a log in for certain elements of the network. All users are reminded or important information such as guidelines to ensure their accounts and logins stay protected. For example, it is the responsibility of individuals to ensure their passwords are protected by not sharing them with anyone else. Individuals have a duty to protect their passwords and personal network logins and are reminded that they should log off when not using the device. Staff, especially, are also reminded about the importance of changing passwords and reasons behind having elements such as multi-authentication log ins for certain online services. Any attempts to access, destroy or corrupt other users' data or compromise the privacy of others, using technology, is not acceptable. Staff are reminded about the importance of using we-based programmes effectively regarding online safety and security due to the importance of the data that these services provide and hold. For example, Arbor, CPOMS, Office 365, etc. Users are reminded that Grove Vale reserves the right to monitor network activity and communication within sites used for school services. This includes monitoring communications that may be private using the school network.

Misuse of the school network and facilities may result of the use having accounts suspended and potential disciplinary action taken. The servers have measures in place to protect them, back up data and prevent viruses. Data Sys are used frequently to sought advice, report and are the main port of call, in reference to managing the servers. Pupils must not access the server. All users are expected to respect the safeguarding guidelines put in place. They should not attempt to introduce viruses, malicious code, by pass network security or use anything that may cause damage or the system and its users at risk. If there are any breaches of technical safeguards, concealing network identities or gaining unauthorised access to the systems services will be deemed unacceptable. Anyone who knows of users breeching these guidelines must reported to the Online Safety Lead, the head teacher or a member of SLT. Users are also reminded that they must not download any

software/hardware to attempt to use any form of hacking systems to gain access to unauthorised areas.

Internet Access

Online safety training is provided to all staff, governors and children are provided with daily online safety sessions, where they learn about correct behaviours and risks of being online. As mentioned, the internet is used frequently within school via a range of devices and technologies. Every effort is used to protect and safeguard users within the school environment (and at home if using school equipment/accessing the network remotely) and provide them with knowledge in order to stay safe and make suitable choices online. Grove Vale School works alongside Data Sys IT to effectively filter and monitor the use of internet services to minimise potential risks and maximise safeguarding ensure using technology and online services at Grove Vale is as safe as possible.

Grove Vale ensures that children are monitored closely when using technology and online services. However, online safety is taught and shared throughout the curriculum and in a variety of ways within school to support children, staff and Grove Vale's wider circle (parents, carers and governors) in being positive online citizens. It is impossible for staff to look at all device screens at once therefore it is important that pupils are reminded of responsible internet use (seen in our online safety policy) and the acceptable use agreement document. To further support staff in monitoring pupils use and supporting online safety/the acceptable use of technology we are using Senso. This allows staff to monitor access to the internet and view pupil's screens. It also records any issues, which can then be immediately addressed to safeguard pupil's and ensure the acceptable use of both technology and internet access. It also the school to take immediate action and act upon any online issues specific to the school e.g trends.

Throughout their learning of online safety, pupils are taught what to do in a wide variety of scenarios including what to if something appears on screen that they are not sure of or do not like. Pupils are asked to turn the screen off and tell an adult immediately. They are also taught about steps to take at home for example, telling a trusted adult immediately, reporting and gathering evidence with the help of an adult. They are also reminded when using technology and when having access to the internet Access to communication services such as public chatrooms and messaging services is not allowed. However, certain communication services may be used with permission obtained from the headteacher. This may be granted to support educational activity.

Social Networking and Email

All members of staff are provided with access to individual email addresses to use for work purposes. There is the opportunity for children to have email addresses and student Office 365 accounts to support them with their learning especially remotely (if needed). To do this Data Sys are consulted and support setting these up. Effective, respectful and acceptable use of accounts are discussed and shared with all who are provided with an account. If accounts are facilitated, Children's accounts are unable to message each other and can only be used to message staff regarding their work.

Parents and guardians, who want to communicate with school, must follow the communication policy and make use of "Contact Us" via our school website. When communication tools are used, the communication guidance of the school should be followed. Staff should ensure that they exercise professionalism at all times when communicating with anyone via email. Any issues should be reported to the head/deputy head teacher immediately. The school networks filters social networking sites. These should not be attempted to be accessed using the school network unless specific permission is granted via the head. All pupils are taught about the correct usage of social media platforms, including age restrictions, frequently within their online safety learning. It is vital that all parties understand and uphold clear boundaries in reference to communicating online to ensure safeguarding is effective for both staff and children. All members of the school community, including pupils, are expected to demonstrate respect, kindness and responsibility when online. Inappropriate use of devices, platforms and other online services will not be accepted. This includes harassment, impersonation, sharing embarrassing/inappropriate content and inappropriate behaviour/messages within chats (to name a few examples). Both in and out of school, social networking should not be used to bring individuals, Grove Vale staff or the Sandwell LA into disrepute. Again, all users have a responsibility to uphold these standards and should report any misuse of technology or unacceptable behaviour of others.

WIFI

Devices within school are connected securely using passwords and are secured by Data Sys. Where possible, safety elements such as multi factor authentication are used. Personal devices should only be connected to the wifi with permission from the head teacher and must adhere to the same rules set for school devices. Visitors to the school must have permission to access the website and must fill in their own acceptable use agreement to do so.

Communication Devices

Staff should not communicate with parents/carers or children via their own personal mobile phones. Staff, who share their personal mobile phone number with pupils/parents, may face a disciplinary action. Communication, as mentioned, must be considered carefully as mentioned and used strictly in a professional manner. Staff and pupils must be aware that under certain circumstances where unacceptable use is suspected enhanced monitoring may take place, including the power to check/confiscate personal technologies. Staff should not use personal telephones to take pictures of pupils.

Cameras/Ipads

Grove Vale encourage the use of media of both staff and pupils in may ways such as assessment, displays, sharing events, for use on the website, etc. However, specific consent should be gained for use for the website, use in the press, etc. This information is collected when children join the school and is checked a number of times throughout their school career at Grove Vale. Consent is collected and recorded on Arbor. 5 Staff may choose to get additional consent for specific things relating to media such as outside agencies using pictures/video, etc. All permission lists follow guidance in accordance to GDPR.

Printing and Photocopying

Staff should not share their account details or passwords for photocopying. They should ensure that when they have finished using the devices they are logged out of them. Printing can be tracked from PaperCut by the office manager. Exceptions may be made if a staff member has asked another to collect printing/copy. However, they should not to this without the account holder's permission.

Computers/Laptops/IPads

Devices are provided to staff in order for them to complete their job role efficiently. Staff must continue to follow guidelines in and out of school. Equipment specifically provided to staff for their use may also be taken off site for staff to complete school work at home. Staff sign a loan agreement, which is kept in the main office. Individual staff, which the equipment if signed out to are responsible for their equipment and the use of them. Data Sys are consulted with to set up the devices and install any software that is required. This includes software instillation and when software needs uninstalling. Any IT issues may be logged with Data Sys using the IT form on Office 365.

Storage

All users are able to save their documents and files within their own areas. There is also areas where users can collaborate together, including the use of Office 365. Staff are encouraged not to use USB devices and instead use the cloud. If they need to use USBs they must use an encrypted device.

Maintenance of Technology

Support of for technology and online services is provided by Data Sys. Their role is key to ensuring facilities at the school work effectively. All users have a duty to report any issues. It is everyone's role to ensure that they use the network responsibly. Also, Data Sys are key to setting up any new technology and ensuring these are safe to use and are secured to protect the school and its users.

AI and Deepfakes

Grove Vale recognises that artificial intelligence (AI) can provide valuable opportunities to support t eaching and learning. However, all AI tools must be used responsibly, safely and in accordance with s chool safeguarding and data protection procedures.

AI platforms must be approved by the school for school related activities and must not enter identifiable pupil information, safeguarding records, confidential documents or sensitive personal data into unapproved systems. AI generated content must be checked for accuracy, suitability, bias and copyright considerations before being used or shared. Pupils must only access AI tools when authorised and appropriately supervised by staff, taking acc ount of age restrictions and educational suitability.

The creation, alteration or distribution of images, audio or video intended to impersonate, humiliate, intimidate, deceive or harm another individual is strictly prohibited.This includes AIgenerated or digi

tally manipulated content involving pupils, staff or members of the school community. Any concerns regarding such content must be reported immediately and safeguarding procedures should be followed.

Reporting

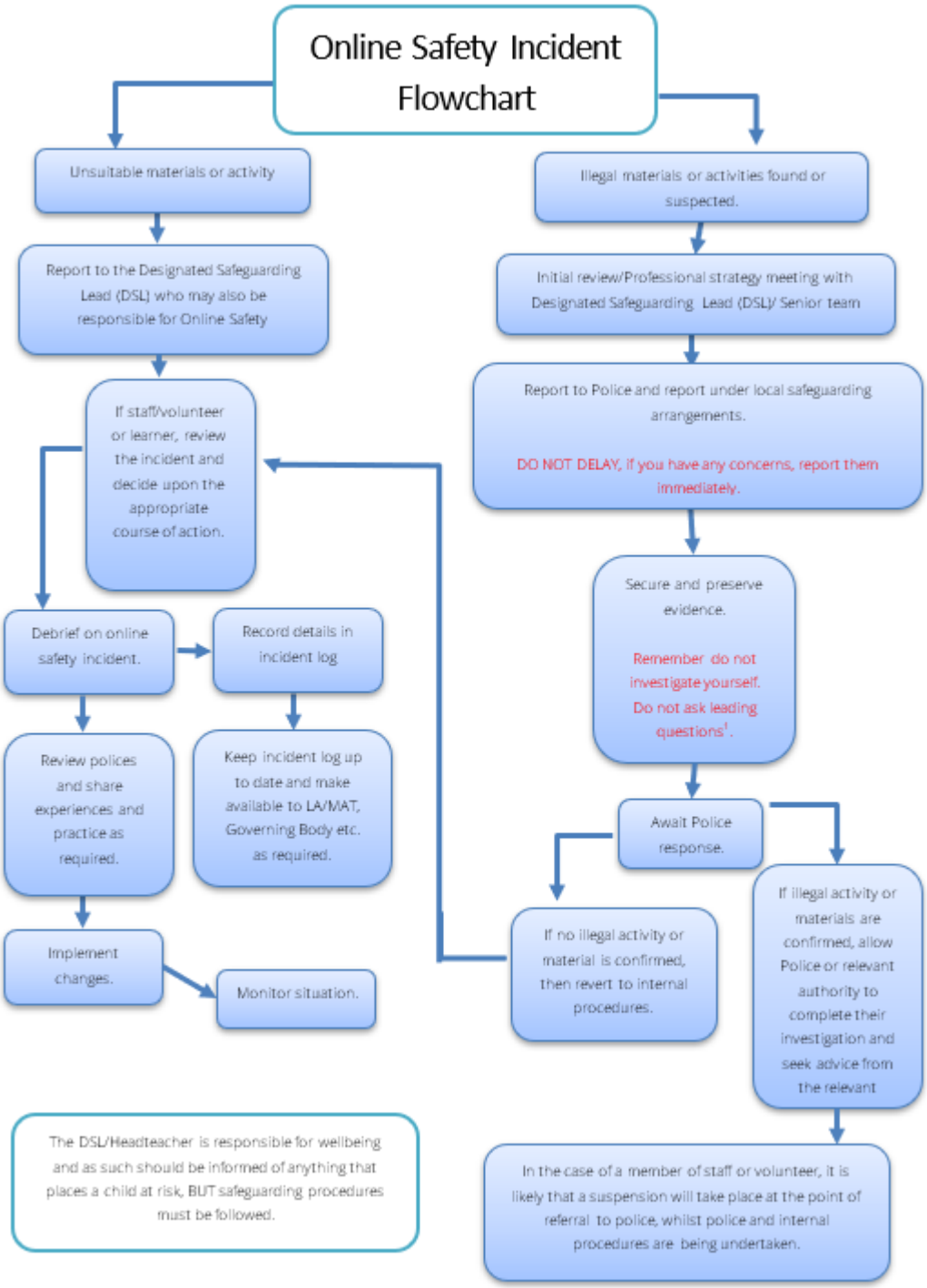
Information regarding reporting incidents needs to be recorded on CPOMMS immediately. Evidence (if possible) should be recorded alongside this within the incident report. Steps should be put into place to address the incident. Staff with follow reporting routes and SLT will be involved with this, including DSL, where necessary. All children and staff are made aware of reporting routes in school as incidents should be dealt with as soon as possible and next steps put into place.

If content involves or there is suspicion of material involving the following:

- Non-consensual images
- Self-generated images
- AI generated (including edited, adapted) harmful content/material
- Inappropriate content including the misuse of AI
- Deep fakes
- Terrorism/extremism
- Hate crime/ Abuse
- Fraud and extortion
- Harassment/stalking
- Child Sexual Abuse Material (CSAM)
- Child Sexual Exploitation Grooming
- Pornography
- Sale of illegal materials/substances
- Cyber or hacking offences under the Computer Misuse Act
- Copyright theft or piracy

safeguarding procedures should be followed. Each incident needs to be assessed in relation to this to ensure that children, staff and parents are safeguarded and the correct action is taken.

If the issues involve staff, then the headteacher should be made aware. If issues involve the head teacher, this should be referred to the chair of governors. Staff should also be aware of relevant external sources that may be utilised for further guidance e.g CEOP.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police 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 ask leading questions[1].
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
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.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.