Whitestone Primary School

Digital Resilience Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users and Governors who have access to and are users of school digital systems, both in and out of the school.

Development/Monitoring/Review of this Policy

This digital resilience policy has been shared with and developed by a working committee made up of:

- *Headteacher (BP)*
- *Senior leadership team (RK and CJ)*
- *Digital Competency and Digital resilience coordinator (JT)*
- *Staff – including practitioners and support staff*
- *Digital resilience group (JT, MG, GA, AH)*
- *Governors (AT)*
- *Parents and carers*

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

Schedule for Development/Monitoring/Review

This digital resilience policy was approved by the Governing body on:	*December 2022*
The implementation of this digital resilience policy will be monitored by:	*Jessica Tanner (DC and digital resilience coordinator)*
Monitoring will take place at regular intervals:	*Termly*
The Governing Body will receive a report on the implementation of the digital resilience policy generated by the monitoring group (which will include anonymous details of digital resilience incidents) at regular intervals:	*Termly*
The digital resilience policy will be reviewed triennually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to digital resilience or incidents that have taken place. The next anticipated review date will be:	*Autumn Term 2025*
Should serious digital resilience incidents take place, the following external persons/agencies should be informed:	*Safeguarding Officer (Bethan Peterson) / LA ICT manager (Chris Rees) / LA safeguarding officer / Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys/questionnaires of*
    - *Learners*
    - *parents and carers*
    - *staff.*

Roles and Responsibilities

The following section outlines the digital resilience roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the digital resilience policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body after receiving regular information about digital resilience incidents and monitoring reports. A member of the Governing Body will take on the role of digital resilience governor and will:

- hold regular meetings with the Digital Competency and digital resilience co-ordinator
- regularly monitor digital resilience incident logs
- regularly monitor filtering change control logs (where possible)
- report to the Governing Body.

Headteacher (BP) and senior leaders

- The Headteacher (BP) has a duty of care for ensuring the safety (including digital resilience) of members of the school community, though the day to day responsibility for digital resilience may be delegated to the Digital Competency and digital resilience co-ordinator (JT)
- The Headteacher (BP) and the senior leadership team should be aware of the procedures to be followed in the event of a serious digital resilience allegation being made against a member of staff
- The Headteacher (BP) and senior leadership team are responsible for ensuring that the Digital Competency and digital resilience co-ordinator (JT) and other relevant staff receive suitable training to enable them to carry out their digital resilience roles and to train other colleagues, as relevant
- The Headteacher (BP) and senior leadership team will receive regular monitoring reports from the Digital Competency and digital resilience co-ordinator (JT)
- The Headteacher (BP) and senior leadership team will ensure that there is a system in place to allow for monitoring
- The Headteacher (BP) and senior leadership team will support those in the school who carry out the internal digital resilience monitoring role.

The Headteacher (BP) should also be trained in digital resilience 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
- cyber-bullying.

Digital Competency and Digital resilience co-ordinator (JT)

The DC and digital resilience co-ordinator:

- leads the digital resilience group
- takes day to day responsibility for digital resilience issues and has a leading role in establishing and reviewing the school digital resilience policies/documents

- ensures that all staff are aware of the procedures that need to be followed in the event of a digital resilience incident taking place
- provides (or identifies sources of) training and advice for staff
- liaises with the local authority
- liaises with school technical staff
- receives reports of digital resilience incidents and creates a log of incidents to help prepare for future digital resilience developments
- meets regularly with the digital resilience governor to discuss current issues, review incident logs and if possible, filtering change control logs
- attends relevant meeting/sub-committee of governors
- reports regularly to the Headteacher (BP) and senior leadership team.

Network manager/technical staff (Local Authority)

The network manager/technical staff (or managed service provider) is responsible for ensuring:

- that the school technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets (as a minimum) the required digital resilience technical requirements as identified by the local authority or other relevant body and also the digital resilience policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with digital resilience technical information in order to effectively carry out their digital resilience role and to inform and update others as relevant
- that the use of the *network/internet/learning platform/Hwb/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher (BP) and Digital Competency and digital resilience co-ordinator (JT) for investigation/action/sanction
- that (if present) monitoring software/systems are implemented and updated as agreed in school policies
- that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of digital resilience matters and of the current school digital resilience policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Headteacher (BP) and Digital Competency and digital resilience co-ordinator (JT) for investigation/action
- all digital communications with learners/parents and carers should be on a professional level and only carried out using official school systems
- digital resilience issues are embedded in all aspects of the curriculum and other activities
- learners understand and follow the digital resilience and acceptable use agreements

- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc., in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned 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.

Digital resilience group

The digital resilience group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding digital resilience and monitoring the digital resilience policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body. The group is made up of two teaching assistants (one based in Foundation Phase and one based in Key Stage 2) and two class teachers (one based in Foundation Phase and one based in Key Stage 2).

Members of the digital resilience group will assist the Digital Competency and digital resilience co-ordinator with:

- the production/review/monitoring of the school digital resilience policy/documents
- mapping and reviewing the digital resilience curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/incident logs where possible
- consulting stakeholders – including parents/carers and the learners about the digital resilience provision
- monitoring improvement actions identified through use of the 360 degree safe Cymru self-review tool.

A digital resilience group terms of reference template can be found in the appendices.

Learners

Learners:

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement
- need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good digital resilience practice when using digital technologies out of school and realise that the school's digital resilience policy covers their actions out of school if related to their membership of the school.

Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters,

school website, Hwb, learning platform and information about national/local digital resilience campaigns/literature. Parents and carers will be encouraged to support the school in promoting good digital resilience practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the school website, Hwb, learning platform and online learner records
- their children's personal devices in the school (where this is allowed).

Community Users

Community users who access school systems/website/Hwb/learning platform as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems. A community users acceptable use agreement template can be found in the appendices.

Policy Statements

Education – learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in digital resilience is therefore an essential part of the school's digital resilience provision. Learners need the help and support of the school to recognise and avoid digital resilience risks and build their resilience.

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

- A planned digital resilience curriculum across a range of subjects, (e.g. ICT/PSE/DCF) and topic areas and should be regularly revisited
- Key digital resilience messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Learners should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Under the Counter Terrorism and Securities Act 2015, schools are required to ensure that children are safe from terrorist and extremist material on the internet
- Learners should be helped to understand the need for the learner acceptable use agreement and 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 monitoring the content of the websites they visit
- It is acceptable that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the technical staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents and carers

Many parents and carers have only a limited understanding of digital resilience 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 therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, school website, learning platform, Hwb
- Parents and carers evenings/sessions
- High profile events/campaigns, e.g. Safer Internet Day
- Reference to the relevant web sites/publications, *e.g.* hwb.wales.gov.uk / www.saferinternet.org.uk / www.chilMGet.com/parents-and-carers (see appendix for further links/resources).

Education – the wider community

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

- Providing family learning courses in use of new digital technologies, digital literacy and digital resilience
- Digital resilience messages targeted towards grandparents and other relatives as well as parents
- The school learning platform, Hwb, and the school website will provide digital resilience information for the wider community
- Supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their digital resilience provision (*e.g.* using Online Compass, an digital resilience self-review tool – www.onlinecompass.org.uk).

Education and training – staff/volunteers

It is essential that all staff receive digital resilience training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal digital resilience training will be made available to staff. This will be regularly updated and reinforced. An audit of the digital resilience training needs of all staff will be carried out regularly. It is expected that some staff will

identify digital resilience as a training need within the performance management process.

- All new staff should receive digital resilience training as part of their induction programme, ensuring that they fully understand the school digital resilience policy and acceptable use agreements.
- The Digital Competency and digital resilience co-ordinator (JT) will receive regular updates through attendance at external training events, (e.g. from Consortium/SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This digital resilience policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days.
- The Digital Competency and digital resilience co-ordinator (JT) will provide advice/guidance/training to individuals as required.

Training – Governors

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

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

Technical – infrastructure/equipment, filtering and monitoring

If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the digital resilience measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school digital resilience policy/acceptable use agreements. The school should also check their local authority/other relevant body policies on these technical issues if the service is not provided by the authority.

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements (these may be outlined in local authority/other relevant body policy and guidance)
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices
- All users will be provided with a username and secure password by the Digital Competency and digital resilience co-ordinator. This person will keep an up to date

record of users and their usernames. Users are responsible for the security of their username and password.

- The "master/administrator" passwords for the school digital systems, used by the network manager (or other person) must also be available to the Headteacher (BP).
- The Headteacher (BP) and Digital Competency and digital resilience co-ordinator (JT) are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (inadequate licencing could cause the school to breach the Copyright Act which could result in fines or unexpected licensing costs)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced/differentiated user-level filtering allowing different filtering levels for different groups of users: staff/learners
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Where possible, school technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc., from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreed policy is in place regarding the extent of personal use that users (staff/learners/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud based services such as email 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 digital resilience education programme.

In preparing a mobile technologies policy the school should consider possible issues and risks. These may include: security risks in allowing connections to your school network; filtering of personal devices; breakages and insurance; access to devices for all learners; avoiding potential classroom distraction; network connection speeds, types of devices; charging facilities; total cost of ownership. A range of mobile technology implementations is possible.

For further reading, please refer to "Bring your own device: a guide for schools/colleges" by Alberta Education available at: http://education.alberta.ca/admin/technology/research.aspx and to the "NEN Technical Strategy Guidance Note 5 – Bring your own device" - http://www.nen.gov.uk/bring-your-own-device-byod/

- The school acceptable use agreements for staff, learners, parents and carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices			Personal Devices		
	School owned for individual use	School owned for multiple users	Other authorised device	Student owned	Staff owned	SLT Staff owned
Allowed in school	Yes (teachers can use laptops for planning, preparation and assessment)	Yes	Yes	No	Yes	Yes
Full network access	No (only SLT logins)	No	No	No	No	No
Internet only	Yes (but filtered)	Yes (but filtered)	Yes (but filtered)	No	No	No
No network access	No	No	No	Yes	Yes	Yes

Using school owned devices

- School owned devices can be used on school premises by staff, learners, Governors and visitors once they have read and signed the acceptable use agreement (AUA).
- All school owned devices must be returned to their designated charging station in the exact same condition and be plugged in to charge. Some devices will be allocated to classrooms and class teachers are responsible for ensuring that their devices are

returned and placed on charge. The majority of the school owned devices will be stored in a charging trolley or charging dock in a locked room.

- If any equipment seems to be damaged or malfunctioning, all stakeholders are required to report the fault to the Digital Competency and digital resilience officer (JT) so that it can be logged and recorded.
- Learners will be prohibited from using a school owned device without adult supervision. Parents/guardians will be informed and potentially held accountable for cost of repairs if their child has caused intentional damage.
- Using school devices for personal use is prohibited, unless it has been granted by the Headteacher (BP), member of the SLT or Digital Competency and digital resilience officer (JT).
- Staff are allowed to take a school owned device home to use for work-related purposes, such as PPA or Microsoft Teams meetings. This request must first be granted by either the Headteacher (BP), member of the SLT or the Digital Competency and digital resilience officer (JT). Staff are responsible for the condition of the device and will be held accountable for loss or damages. Staff will be required to pay for the cost of replacement or repair.
- All installations of apps, changes to settings, requests for replacements or repairs will be overseen and managed by the Digital Competency and digital resilience officer (JT).
- All technical support for school owned devices will be requested by the Headteacher (BP) or Digital Competency and digital resilience officer (JT) and overseen by the Local Authority IT Team.
- All users must be made aware of Data Protection precautions. All users can use their personal login details when accessing safe websites, but **must not save their login details**.
- Staff are required to check devices for any inappropriate use. Any users will be liable for any images, downloads, videos or websites accessed or created inappropriately.
- In the instance that learners cannot access a device at home, parents/guardians are able to request to loan a school owned device. Once granted by the Headteacher (BP) and the Digital Competency and digital resilience officer (JT), learners will be able to use the school owned device for educational purposes only. Parents/guardians are responsible for the condition of the device and will be held accountable for loss or damages. Parents/guardians will be required to pay for the cost of replacement or repair.

Using personal devices

- Learners are prohibited from using their personal devices in school. If they need to bring their personal device to school (perhaps to communicate with their parents/guardians when they walk home from school), then their device must be handed into the school office where it will be safely secured until the end of the school day.
- Visitors are asked not to use their personal device during lesson times when in the presence of learners.
- Staff are able to access and use their personal device during lesson times if they are picturing learners or learners' work (to be printed or uploaded to the school Twitter page). Staff are required to delete images and videos immediately after they have printed, transferred or shared them appropriately.
- Staff are prohibited from using their personal devices during working hours for personal reasons. However, if staff have extenuating circumstances (such as a family issue),

these must be communicated to the Headteacher (BP) and SLT so that reasonable tolerances can be made (such as allowing a staff member to take a phone call regarding a family member).

- Staff are responsible for their own personal devices and the school is not liable for any loss or damages.
- Staff are responsible for the appropriate use of their personal device for work-related purposes. Staff are prohibited from leaving their personal device with learners unsupervised. Staff must be cautious of their personal usage being exposed to learners, such as their personal messages, their screensaver, their apps or their browser history.

Teams Meetings between staff and pupils at home

During time at home, teachers can organise Teams Meetings (via the children's Hwb accounts) with pupils for check-in and safeguarding purposes. In order to set up Teams Meetings between staff and pupils whilst they are at home, it has been agreed that:

- Parents/guardians must give consent prior to being invited to join a Teams Meeting
- At all times, there must be two staff members present on a Teams Meeting call
- Children must not be in Teams Meeting without two staff members present - both staff members must join the meeting prior to the children and must not leave the meeting until all the children have left and closed down Teams
- Staff and pupils are permitted to change their background prior to the meeting if they would prefer maintaining their privacy whilst calling from their home
- Teams Meetings can involve no more than five pupils
- Teams Meetings should last between 5 and 20 minutes
- The Meeting Organiser (the class teacher) is permitted to mute other members' microphones, e.g. if the noise disruption is interfering with members talking
- During the meeting, the staff can ask the children questions about their time at home or encourage the children to engage with games
- Parents or guardians can also be present with their child on the video but must display appropriate behaviour and language throughout the duration of the meeting.