Bradshaw Hall Primary School

E-SAFETY POLICY – ICT & iPAD ACCEPTABLE USER POLICY

Bradshaw Hall Primary School
Vernon Close,
Cheadle Hulme,
SK8 6AN

Date Reviewed:	**Autumn 2023**
Date Ratified & Adopted by the Governing Board:	**Autumn 2023**
Signed - Head Teacher	
Signed - Chair of Governing Board	
Next Review:	**Autumn 2024**
Comments:	**Adapted & Adopted from Local Authority model policy Spring 2018** **COVID Addendum removed**

BRADSHAW HALL PRIMARY SCHOOL

Development / Monitoring / Review of this Policy

This e-safety policy has been developed through consultation with the range of stakeholders list below. Collectively they are referred to as the E-Safety Monitoring Group:

- *Headteacher & Senior Leaders*
- *E-Safety Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *School Council*
- *Governing Board*
- *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 e-safety policy was first approved by the *Governing Board*	*Autumn 2016*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Monitoring Group*
Monitoring will take place at regular intervals:	*Each Half Term*
Governing Board / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	*Each Term*
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*Annually during the Autumn Term*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager – Damien Hodgkinson, Local Area Designated Officer - LADO (Safeguarding Officer), Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
    - *pupils*
    - parents / carers
    - *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The 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 e-safety behaviour that take place out of school.

Roles and Responsibilities

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

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Board Teaching & Learning Sub Committee, receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Board has taken on the role of *E-Safety* Governor. The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *regular monitoring of filtering / change control logs*
- *reporting to relevant Governors / Board / committee / meeting*
- *ensure that school systems and equipment is not used for the promotion of terrorism and /or violent extremism activities*

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**.
- **The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.** (see flow chart on dealing with e-safety incidents – included in "Responding to incidents of misuse" and the relevant *Local Authority HR* disciplinary procedures)
- **The Headteacher will ensure that all staff maintain an upto date work knowledge of the PREVENT agenda and processes for preventing the promotion of radicalisation and violent extremism ideologies through providing for regular updates and training**
- The Headteacher & Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Headteacher and senior leaders will provide and review annually an Acceptable Use Procedure and Code of Conduct for all staff
- The school will agree a 'buy-back' Service Level Agreement – SLA, from AVA Services provided by the LA. This will include Fire Wall protection, first line filtering for inappropriate and undesirable material and Forensic Analysis of internet and email use.
- The Senior Leadership Team will undertake regular monitoring of e-safety and report to staff & governors

E-Safety Coordinator:

The current Designated Safeguarding Leads will oversee the half-termly data monitoring with the day-to-day responsibility for e-safety led by C B**agnall & *R Gleaves***. Key responsibilities will be to:

- lead the e-safety committee
- take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- maintain an appropriate level of knowledge and training with regard to ICT use and misuse so as to fulfil the role
- provide training and advice for staff
- liaise with the Local Authority / relevant body
- liaise with school technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform the Headteacher & future e-safety developments,
- meet regularly with E-Safety Governor to discuss current issues and review incident logs
- attend relevant committee meetings with Governors
- report regularly to Senior Leadership Team

Network Manager / Technical staff:

The SMBC Network Manager is responsible for ensuring:

- **that the school's technical infrastructure is secure and is not open to misuse or malicious attack**
- **that the school meets required e-safety technical requirements and any *Local Authority / other relevant body* E-Safety 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**
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the *network / internet / intranet / Virtual Learning Environment / remote access & email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *Headteacher; E-Safety Coordinator* for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in the school's policies

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)**
- **they report any suspected misuse or problem to the *Headteacher/Leader ; E-Safety Coordinator for* investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems**
- **e-safety issues are embedded in all aspects of the curriculum and other activities**

- **students / pupils understand and follow the e-safety and acceptable use policies**
- **students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations**
- **they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices**
- **in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches**

Child Protection / Safeguarding Designated Persons:

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- accessing racist and violent extremist materials

E-Safety Group

The E-Safety Group provides a consultative group that has wide representation from the school with responsibility for issues regarding e-safety and the monitoring of the e-safety policy, including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Board.

Members of the E-safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- **are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy below**
- will 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 e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Pupils Acceptable User Policy

1) *Don't post any personal information online – like your address, email address or mobile number.*
2) *Think carefully before posting pictures or videos of yourself. Once you've put a picture of yourself online, most people can see it and may be able to download it, it's not just yours anymore.*
3) *Keep your privacy settings as high as possible*
4) *Never give out your passwords*
5) *Don't befriend people you don't know*
6) *Don't meet up with people you've met online. Speak to your parent or carer about people suggesting you do*
7) *Remember, that not everyone online is who they say they are*
8) *Think carefully about what you say before you post something online*
9) *Respect other people's views, even if you don't agree with someone else's views doesn't mean you need to be rude*
10) *If you see something online that makes you feel uncomfortable, unsafe or worried: leave the website, turn off your computer if you want to and tell a trusted adult immediately*

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

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

Community Users

It is not envisaged that members of the community will ordinarily have access to, either regularly or irregularly, the school's network, computers (including ancillary equipment e.g. iPads), or any other part of the electronic system to access school data files, records or internet use.
Any changes to this commitment will need to be agreed by the full Governing Board after consultation and deliberation.

Policy Statements

Education – pupils

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

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

- **A planned e-safety curriculum will be provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities**
- **Students / pupils will be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Students / pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- *Pupils* **will** *be helped to understand the need for the* ***Pupil Acceptable Use Agreement*** *and encouraged to adopt safe and responsible use both within and outside school*
- *Staff* **will** *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 pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff* **will** *be vigilant in monitoring the content of the websites the young people visit.*
- *It is accepted that from time to time, for good educational reasons, students 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 LA 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 / carers

Many parents and carers have only a limited understanding of e-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 on-line 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, web site, VLE*
- *Parents / Carers evenings / sessions*
- *High profile events / campaigns e.g. Safer Internet Day*
- *Reference to the relevant web sites / publications e.g.* *www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.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 / e-safety knowledge and experience. This may be offered through the following:

- *Providing family relative information in the use of new digital technologies, digital literacy and e-safety*
- *E-Safety messages targeted towards parents, grandparents and other relatives as well as parents.*
- *The school website will provide e-safety information and web-site links for the wider community*
- *Supporting enquiring community groups e.g. Early Years Settings, Child-minders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk*

Education & Training – Staff / Volunteers

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

- **A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly** SWGfL BOOST includes unlimited online webinar training for all, or nominated, staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development) *It is expected that some staff will identify e-safety as a training need within the performance management process.*
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.** SWGfL BOOST includes an array of presentations and resources that can be presented to new staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources)
- *The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

  SWGfL BOOST includes an array of presentation resources that the e-Safety coordinator can access to deliver to staff (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Resources). It includes presenter notes to make it easy to confidently cascade to all staff

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / e-safety / health and safety / child protection. 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

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 ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements outlined in the Local Authority policy and guidance**
- **There will be regular reviews and audits of the safety and security of school academy 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** (at KS2 and above) **will be provided with a username and secure password** by *AVA Services who will keep an up to date record of users and their usernames.* **Users are responsible for the security of their username and password** *and will be required to change their password when advised by AVA Services*
- **The "master / administrator" passwords for the school / academy ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher / Principal* or other nominated senior leader and kept in a secure place (e.g. school safe)**
- Mrs K Lee **is 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 (e.g. 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. In addition, the school will employ the AVA Services Forensic Analysis service through a SLA to further monitor and report on inappropriate and unacceptable use of ICT systems from spring 2017. 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 ages / stages and different groups of users – staff / pupils / students etc.)
- *AVA 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.* (schools may wish to add details of the monitoring programmes that are used).
- *An appropriate system is in place through the **Note of Concern** system of reporting for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).*
- Appropriate security measures are in place through AVA Services & Forensic Data Monitoring via SMBC 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. All staff sign the schools agreement to abide by the schools Codes of Conduct & Acceptable Use Policies & Procedures for use of computers, iPods, iPads and use of the internet.
- *An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school in as much as a member of staff must seek agreement from the Headteacher which must be granted in all cases. (See also: Managing Personal & Sensitive Information in Schools)*
- *An agreed policy is in place that 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. See also: Managing Personal & Sensitive Information in Schools)*

Bring Your Own Device (BYOD)

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. However, there are a number of e-safety considerations for BYOD that need to be reviewed prior to implementing such a policy. Use of BYOD should not introduce vulnerabilities into existing secure environments. Considerations will need to include; levels of secure access, filtering, data protection, storage and transfer of data, mobile device management systems, training, support, acceptable use, auditing and monitoring. This list is not exhaustive and a BYOD policy should be in place and reference made within all relevant policies.

Bradshaw Hall Primary School endeavors to provide sufficient hardware PC's, laptops and other mobile devices for use in school and therefore does not permit the use of Bring Your Own Device (BYOD) for use in school at any time.

Use of Digital and Video Images

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

- **When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites**
- 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 *pupils* 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, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.*
- *Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Pupils' 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 pupils are published on the school website*
- *Pupil's work can only be published with the permission of the pupil and parents or carers.*

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Following a number of "high profile" losses of personal data by public organisations, schools are likely to be subject to greater scrutiny in their care and use of personal data. A School Personal Data template is available in the appendices to the appendices version of this document.

The school ensures that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".**
- **School has a Data Protection Policy (see DP/GDPR Policies)**
- **School is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.**
- **Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.**
- **Transfer data using encryption and secure password protected devices.**

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory stick/cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Not Allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to the school		X					X	
Use of mobile phones in lessons	X				X			
Use of mobile phones in social time for personal use			X		X			
Taking photos on personal mobile phones / cameras	X				X			
Use of other mobile devices i.e. iPad/tablets			X				X	
Use of personal email addresses in school or on school network				X	X			
Use of school email for personal emails	X				X			
Use of messaging apps			X		X			
Use of social media on school network	X				X			
Use of blogs			X					

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 pupils should therefore use only the school / academy email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school policy, 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.** (SWGfL BOOST includes an anonymous reporting app Whisper - http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/SWGfL-Whisper)

- **Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc.) 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.*
- *Whole class / group email addresses may be used at KS1, while pupils at KS2 and above will be provided with individual school email addresses for educational use.*
- *Students / pupils should be taught about e-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.*
- *Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.*

Social Media - Protecting Professional Identity

With an increase in use of all types of social media for professional and personal purposes a policy that sets out clear guidance for staff to manage risk and behaviour online is essential. Core messages should include the protection of pupils, the school and the individual when publishing any material online. Expectations for teachers' professional conduct are set out in 'Teachers Standards 2012'. While, Ofsted's e-safety framework 2012, reviews how a school protects and educates staff and pupils in their use of technology, including what measures would be expected to be in place to intervene and support should a particular issue arise.

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

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues. SWGfL BOOST includes unlimited webinar training on this subject: (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Professional-Development)
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff will ensure that:

- No reference is made in social media to pupils, 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.
SWGfL BOOST includes SWGfL Alerts that highlight any reference to the school/academy in any online media (newspaper or social media) for example http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Alerts

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

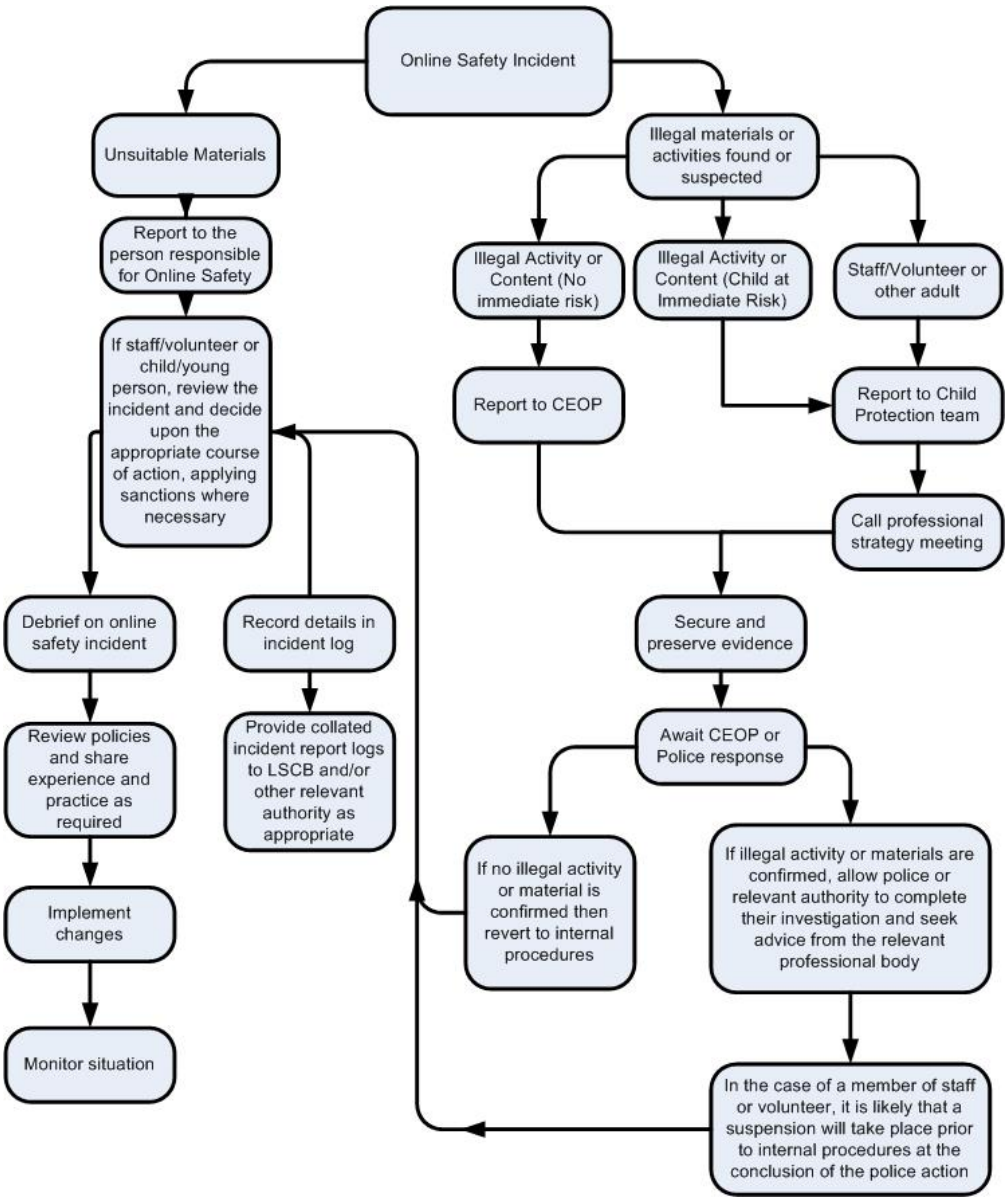
		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Which promotes or glorifies Radicalisation and/or Violent Extremism					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. X financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)				X		
On-line gaming (non-educational)					X	
On-line gambling					X	
On-line shopping / commerce					X	
File sharing				X		
Use of social media				X		
Use of messaging apps				X		
Use of video broadcasting e.g. YouTube				X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above). SWGfL BOOST includes a comprehensive and interactive 'Incident Management Tool' that steps staff through how to respond, forms to complete and action to take when managing reported incidents (http://www.swgfl.org.uk/Staying-Safe/E-Safety-BOOST/Boost-landing-page/Boost-Hub/Incident-Response-Tool)

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

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

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

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

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

School Actions & Sanctions

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 as follows:

Pupils — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Head of Key Stage	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X		
Unauthorised use of non-educational sites during lessons		X	X						
Unauthorised use of mobile phone / digital camera / other mobile device		X	X						
Unauthorised use of social media / messaging apps / personal email			X						
Unauthorised downloading or uploading of files			X						
Allowing others to access school network by sharing username and passwords			X						
Attempting to access or accessing the school network, using another pupil's account			X						
Attempting to access or accessing the school / academy network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						
Continued infringements of the above, following previous warnings or sanctions			X	X					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
Using proxy sites or other means to subvert the school's filtering system			X						
Accidentally accessing offensive or pornographic material and failing to report the incident			X						
Deliberately accessing or trying to access offensive or pornographic material			X	X					
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X						

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email		X	X					
Unauthorised downloading or uploading of files		X	X					
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X	X					
Careless use of personal data e.g. holding or transferring data in an insecure manner		X	X					
Deliberate actions to breach data protection or network security rules		X	X	X				
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X				
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					
Actions which could compromise the staff member's professional standing		X	X					
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X					
Using proxy sites or other means to subvert the school's filtering system		X	X					
Accidentally accessing offensive or pornographic material and failing to report the incident		X						
Deliberately accessing or trying to access offensive or pornographic material		X	X	X				
Breaching copyright or licensing regulations		X	X					
Continued infringements of the above, following previous warnings or sanctions		X	X	X				

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be downloaded from:

http://www.swgfl.org.uk/Staying-Safe/Creating-an-E-Safety-policy

Acknowledgements

SWGfL would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this School E-Safety Policy Template and of the 360 degree safe E-Safety Self Review Tool:

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Representatives of SW Local Authorities
- Plymouth University Online Safety
- NEN / Regional Broadband Grids

NEXT SECTION CONTAINS:

THE STAFF CODE OF CONDUCT FOR ICT & iPAD USE PROCEDURE (ACCEPTABLE USER POLICY - AUP)

Bradshaw Hall Primary School

Staff Code of Conduct for ICT & iPad Use Procedure

Bradshaw Hall Primary School
Vernon Close,
Cheadle Hulme,
SK8 6AN

Date Reviewed:	**Autumn 2023**
Date Ratified & Adopted by the Governing Board:	**Autumn 2023**
Signed - Head Teacher	
Signed - Chair of Governing Board	
Next Review:	**Autumn 2024**
Comments:	**Adapted & Adopted from Local Authority model policy Spring 2018** **COVID Addendum removed**

Bradshaw Hall Primary School

Staff Code of Conduct for ICT & iPad Use Procedure

I understand this document is taken from the school's E-Safety Policy document which I have read

The purpose of the code of conduct is to provide guidance about safer working practice, keeping my personal and private lives separate, keeping myself safe when using electronic media and adopting responsible behaviour that should prevent me from putting myself and my career at risk.

This document refers to professional working relationships with colleagues, children, young people, parents / carers and volunteers.

I Will Not:

- Give my personal details to children/young people. This includes mobile phone numbers, details of blogs, details of personal websites, social networking accounts, passwords, PIN numbers, Log in Details
- Give my passwords and Log In details to anyone
- Use my personal mobile phone to communicate with children/young people except in genuine emergencies.
- Make available my personal details on a social network site with children/young people. I am aware that belonging to a group may give a back door to my page
- Enter into discussions, make personal comments or express personal views relating to any school activities, either business or social activities, on social media such as Twitter, Facebook, Snapchat, Instagram or similar media which could impact adversely on the school
- Add/allow a child/young person to join my contacts/friends list
- Use the internet or web-based communication to send messages to children/young people un-related to school
- Use my personal e-mail address in any communication with children and young people
- Tick the 'remember me' box when using password protected internet sites in school
- Retain pupil/family contact details for personal use
- Produce images of children and young people unless appropriate permission has been sought
- Use personal computers for the storage or access of school documents or images
- Use school information systems for private purposes without the permission of the Headteacher or designated alternate
- Install any additional hardware or software without the permission of the Headteacher or designated alternate
- Upload or download inappropriate or illegal material, nor assist young people in this process

I Will:

- Only use my mobile phone in line with school policy during directed time
- Always anonymise my mobile phone number if I have to use my phone in an emergency to contact parents, carers or volunteers
- Switch off any blue tooth visibility
- Password protect, switch off and lock my technology when it is not in use
- Ensure that all written communications are compatible with my professional role
- Remember that on-line conversations are written documents and should be treated as such
- Store images of children/young people in the secure network space specified by the school and
- Delete such images from the device as soon as they have been stored whether using my own digital camera (with the permission of the Headteacher) or that of the school
- Remove any contact details of children/young people /parents/carers/volunteers from a mobile device once the activity is complete. This includes school equipment and my personal mobile if permission for its use has been granted
- Respect copyright and intellectual property rights

I Will Consult the Headteacher if:

- I have an existing social relationship with a child/young person/parent/carer / volunteer outside school which leads me to communicate with them using technology
- I have an existing social relationship with a child/young person/parent/carer/ volunteer outside school which leads me to play on-line games with them

I understand the advice listed below:

The Governors and Headteacher recommend that I:

- Set your privacy settings at a maximum for any social network site/image storage etc.
- Make sure that any information that is about me that is publicly available is accurate and appropriate to my professional role
- Are mindful about how you present yourself when you are publishing information about yourself or having conversations on-line
- Assume that **any** information that you post is publicly available

Use of Staff iPad Procedure

Bradshaw Hall Primary School is committed to improving the access to learning and the personal development opportunities of its pupils. We believe the use of the Apple iPad in teaching and learning can help towards these goals and iPads are provided to teaching staff for this reason. By signing below you agree to accept the use of school iPads under the following terms of use:

1. These iPads remain the property of Bradshaw Hall School and are for use **only** by you, support staff and pupils in your class. They must not be loaned to other adults or pupils without agreement from the Headteacher.

2. All iPad users must sign and fully comply with the Bradshaw Hall School ICT Acceptable Usage Policy.

3. These iPads are linked to school systems. Apps should be purchased through the school account ONLY via AVA. No personal information of children or regarding children should be stored on the iPad. Ensure you store to the blog, the Media file or delete the videos or images. You must fully comply with high standards of data protection.

4. Make sure the iPad is password protected and stored with the ICT coordinator. This password can be shared with your support staff.

5. You (and only you) may take the password protected iPad off-site if you plan to use it in a way that will benefit the school. Insurance cover provides protection from the standard risks whilst the iPad is on the school site or in your home **but excludes** theft from your car or from other establishments.

6. Loss or damage of a device should be reported to the Headteacher immediately. If necessary the device will be remotely locked or wiped.

7. Anonymous email and internet activity is possible with these iPads. If the Headteacher has just cause or concern staff and/or pupils may be monitored.

8. iPads should only be used when the teacher believes that all pupils present are capable of using them sensibly and in accordance with the Accepted User Policy and standards.

9. You are responsible for looking after these iPads. When left unattended they must be locked in a secure cupboard in your classroom. Control of the cupboard key is your responsibility. The whereabouts of these iPads should be reported to the ICT coordinator but not be divulged to adults or pupils outside your class team.

10. These iPads are configured with certain restrictions in place. You must not try to make changes to the devices if they are passcode protected.

11. Any connection cost incurred by accessing the internet from outside school is not chargeable to the school.

12. Posts to the blog should always be considered. Whilst the blog has unlimited capacity, it is imperative that children don't have their pictures uploaded unnecessarily.

13. If a video or picture is streamed of a child, it should not be unnecessarily stored on the computer. Make a decision to upload or delete.

14. All Stockport and school policies regarding appropriate use and sharing information apply to all school iPads. Use of the iPad must adhere to data protection, computer misuse and health and safety rules. Failure to do so may lead to disciplinary action.

15. If you leave the employment of the Bradshaw Hall Primary School, the iPads must be returned to the Headteacher. iPads are the property of the school

Extract from the Staff Handbook

PROFESSIONAL CONDUCT

It is expected that all staff and volunteers conduct themselves with the utmost professionalism at all times, both inside school and outside in line with accepted and nationally established professional codes of conduct. Staff should never, under any circumstances, allow themselves to become personally involved in a relationship with any child, neither sexual nor plutonic. Staff must not enter into any arrangement or relationship which would discredit the good name of the school and/or all the staff engaged at the school. Failure to adhere to established professional codes of conduct will result in serious misconduct proceedings being invoked.

I understand a copy of page 6 of this document, which I have signed and dated, is contained within my personnel file.

E-Safety Acceptable User Policy for Staff & Use of Staff iPad Procedure

Please complete and detach page 7 and return to RG. Retain this booklet for your own records.

Please tick

- ☐ I am aware that I must not behave in a way that could suggest that I am trying to develop a personal relationship with a child known to me through my professional role
- ☐ I have read the E-Safety Policy & guidelines produced by Stockport Safeguarding Children Board
- ☐ I will report any incidents of e-safety regarding children/young people to a Designated Child Safeguarding Officer in school
- ☐ I am aware that activities I undertake within my private life using technology may bring the profession/establishment into disrepute
- ☐ I understand that the headteacher may ask to view my school equipment at any time
- ☐ I have read and understand the above ICT e-Safety Code of Conduct and Use of iPad Procedures
- ☐ I have read the schools main E-Safety Policy document which sets out in detail all aspects of E-Safety relating to the school

Signed:

Full Name:

Date:

Detached copy to be stored in personnel file.
This copy to be retained by member of staff

PLEASE COMPLETE THIS PAGE. DETACH & RETURN TO RG

E-Safety Acceptable User Policy for Staff & Use of Staff iPad Procedure

Please tick

- ☐ I am aware that I must not behave in a way that could suggest that I am trying to develop a personal relationship with a child known to me through my professional role
- ☐ I have read the E-Safety Policy & guidelines produced by Stockport Safeguarding Children Board
- ☐ I will report any incidents of e-safety regarding children/young people to a Designated Child Safeguarding Officer in school
- ☐ I am aware that activities I undertake within my private life using technology may bring the profession/establishment into disrepute
- ☐ I understand that the Headteacher may ask to view my school equipment at any time
- ☐ I have read and understand the above ICT e-Safety Code of Conduct and Use of iPad Procedures
- ☐ I have read the schools main E-Safety Policy document which sets out in detail all aspects of E-Safety relating to the school

Signed: Full Name: Date:
Administration use Received By: Role: Date: