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 2024**
Date Ratified & Adopted by the Governing Board:	**Autumn 2024**
Signed - Head Teacher	
Signed - Chair of Governing Board	
Next Review:	**Autumn 2025**
Comments:	**Adapted & Adopted from Local Authority model policy Spring 2018** **COVID Addendum removed** **Significant review by SWGfL & SMBC Safeguarding Partnership Autumn 2024**

Bradshaw Hall Primary School

Scope of the Policy

This Online Safety Policy outlines the commitment of Bradshaw Hall Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice. This school is aware of the legislative framework under which this Online Safety Policy template and guidance has been produced as outlined in the attached 'Legislation' Appendix.

This Online Safety Policy applies to all members of the school community, including staff, learners, governors, volunteers, parents and carers, visitors and community users, who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where permitted).

Bradshaw Hall Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

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*
- *Designated safeguarding Lead*
- *E-Safety Coordinator*
- *Staff – including Teachers, Support Staff, Technical staff*
- *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* The policy is reviewed annually and has been significantly updated by SWGfL & and recommended by SMBC Safeguarding Partnership	*Autumn 2016* Autumn 2024
The implementation of this e-safety policy will be monitored by the:	*E-Safety Monitoring Group & DSL's*
Monitoring will take place at regular intervals:	*Each 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.	*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*

Roles and Responsibilities

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

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 & the Safeguarding Sub-groups, receiving regular information about e-safety incidents and monitoring reports. A member of the Teaching & Learning sub-group has taken on the role of *E-Safety* Governor. The role of the E-Safety Governor will include:

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

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

Headteacher and Senior Leaders:

- *The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education*

[1] In a small school some of the roles described may be combined, though it is important to ensure that there is sufficient 'separation of responsibility' should this be the case.

- *The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[2].*
- *The headteacher/senior leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant*
- *The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role*
- *The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead*
- *The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring*

The DSL's will:

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

[2] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

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 Bagnall & R Gleaves. Key responsibilities will be to:

The Online Safety Leads will:

- *lead the Online Safety Group*
- *work closely on a day-to-day basis ~~with the Designated Safeguarding Lead (DSL),~~ to receive reports of online safety issues, being aware of the potential for serious child protection concerns and ensure that these are logged to inform future online safety developments*
- *have a leading role in establishing and reviewing the school online safety policies/documents*
- *promote an awareness of and commitment to online safety education/ awareness raising across the school and beyond*
- *liaise with ~~curriculum~~ subject leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated*
- *ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents*
- *provide (or identify sources of) training and advice for staff/governors/parents/carers/learners*
- *liaise with (school/local authority/external provider) technical staff, pastoral staff and support staff (as relevant)*
- *receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined within 'Keeping Children Safe in Education':*
    - *content*
    - *contact*
    - *conduct*
    - *commerce*

Subject Leads

Subject Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme e.g. ProjectEVOLVE
This will be provided through:

- *discrete programmes*
- *PHSE and SRE programmes*
- *A mapped cross-curricular programme*
- *assemblies and pastoral programmes*

- *through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week*

Teaching and Support Staff

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

Network Manager / Technical staff:

The DfE Filtering and Monitoring Standards says:

> *Senior leaders work closely with governors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. IT*

services are provided by Stockport LA via AVA Services who provide mainframe and support services with access to a dedicated technician.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The Headteacher and DSL team work closely together with IT service providers to meet the needs of your setting. Specific training and support with filtering and monitoring is received from AVA.

AVA IT Services provides technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems*

AVA IT services support the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

AVA IT Services is responsible for ensuring that:

- *they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy*
- *the school technical infrastructure is secure and is not open to misuse or malicious attack*
- *the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority there is clear, safe, and managed control of user access to networks and devices*
- *they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant*
- *the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to E-Safety Coordinators for investigation and action*
- *the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix C1 'Technical Security Policy template' for good practice).*
- *monitoring systems are implemented and regularly updated as agreed in school policies*

Child Protection / Safeguarding Designated Persons:

is 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 learner acceptable use agreement and Online Safety Policy (this should include personal devices – where allowed)*
- *should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so*
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

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.*
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 and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

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

- publishing the school 'Online Safety Policy' on the school website
- providing them with a copy of the learners' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carer AUA in the appendix A4)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature

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

- *reinforcing the online safety messages provided to learners in school.*
- *the safe and responsible use of their children's personal devices in the school (where this is allowed)*

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 **and** will be expected to sign a community user AUA before being provided with access to school systems. (A community user's acceptable use agreement template can be found in the appendices).

The Online Safety Policy:

- *sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication*
- *allocates responsibilities for the delivery of the policy*
- *is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours*
- *establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world*
- *describes how the school will help prepare learners to be safe and responsible users of online technologies*
- *establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms*
- *is supplemented by a series of related acceptable use agreements*
- *is made available to staff at induction and through normal communication channels such as the staff intranet and during review consultations*
- *is published on the school website*

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

An Acceptable Use Agreement is a document that outlines the school's expectations on the responsible use of technology by its users. Senior leaders request that they are

signed and acknowledged by the staff as part of their conditions of employment. Some may also require learners and parents/carers to sign them, though it is more important for these to be regularly promoted, understood and followed rather than just signed. There is a range of acceptable use agreements in the appendices.

The Online Safety Policy and Acceptable Use Policy defines acceptable use at the school. The Acceptable Use policy will be communicated and re-enforced through:

- *learner handbook*
- *staff induction and handbook*
- *splash screens*
- *digital signage*
- *posters/notices around where technology is used*
- *communication with parents/carers*
- *built into education sessions*
- *school website*
- *peer support*

Schools has discussed and agreed which activities are acceptable/unacceptable. This will vary with the ages of the learners. It is recommended that the school discuss and agree on these activities and to complete the following tables as guidance for members of the school community:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					x
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in cyber-					x

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	crime and harness their activity in positive ways- further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes: Schools may wish to add further activities to this list.	Staff and other adults				Learners			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Online gaming								
Online shopping/commerce								
File sharing								
Social media								

Messaging/chat								
Entertainment streaming e.g. Netflix, Disney+								
Use of video broadcasting, e.g. YouTube, Twitch, TikTok								
Mobile phones may be brought to school								
Use of mobile phones for learning at school								
Use of mobile phones in social time at school								
Taking photos on mobile phones/cameras								
Use of other personal devices, e.g. tablets, gaming devices								
Use of personal e-mail in school, or on school network/wi-fi								
Use of school e-mail for personal e-mails								

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

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a 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.

- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners

Reporting and Responding

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

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

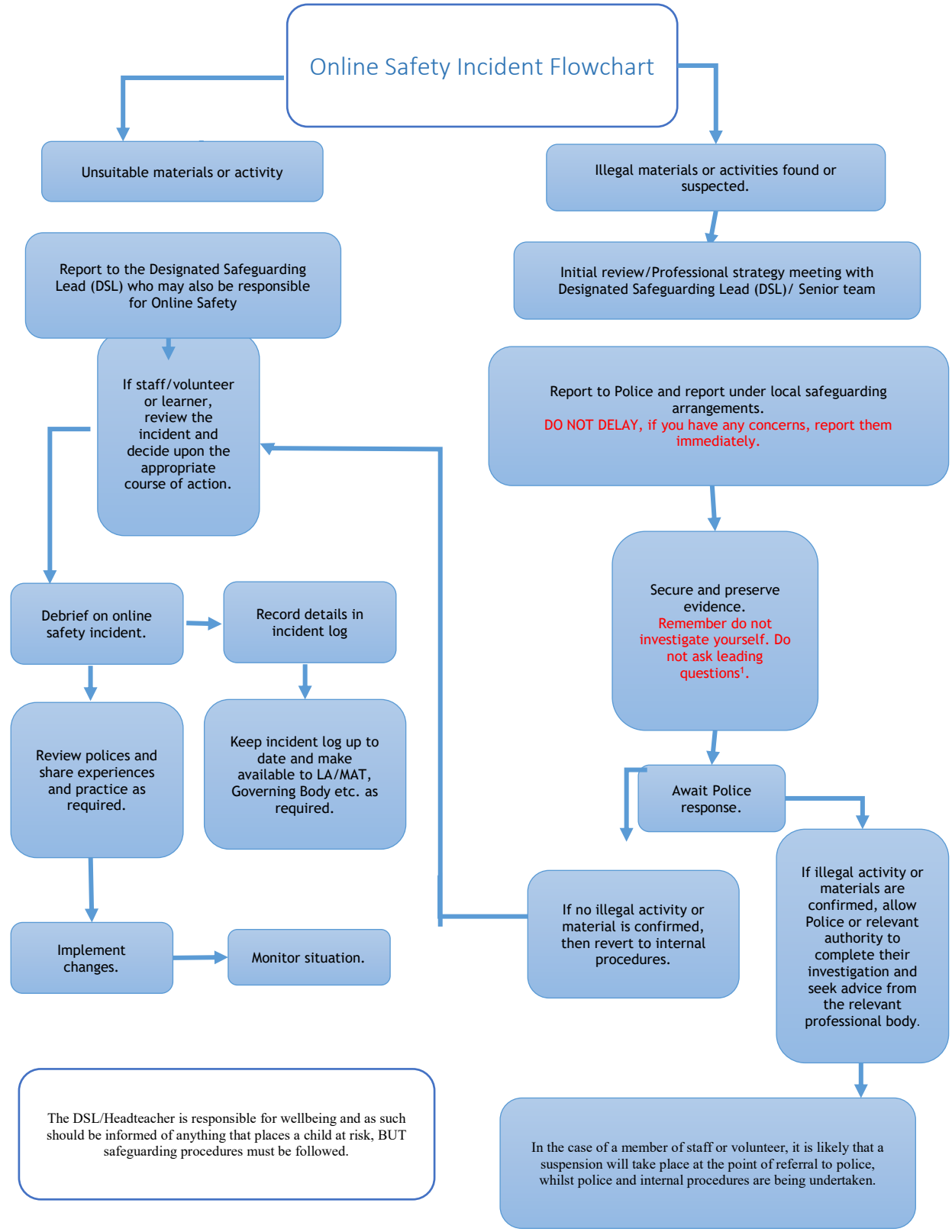
- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. (Schools may wish to consider the use of online/anonymous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

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

- *any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority*
- *where there is no suspected illegal activity, devices may be checked using the following procedures:*
    - *one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.*
    - *conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.*
    - *ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)*
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged (insert details here).
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
    - *the Online Safety Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with*
    - *staff, through regular briefings*
    - *learners, through assemblies/lessons*

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

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


Online Safety Incident Flowchart
Unsuitable materials or activity
Illegal materials or activities found or suspected.
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Debrief on online safety incident.
Record details in incident log
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
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.
Await Police response.
Implement changes.
Monitor situation.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
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.
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.

School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows: (the school will need to agree upon its own responses and place the ticks in the relevant columns. They may also wish to add additional text to the column(s) on the left to clarify issues. Schools have found it useful to use the charts below at staff meetings/training sessions)

Responding to Learner Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Principal Teacher / Deputy Head	Refer to Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device / network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords									
Corrupting or destroying the data of other users.									
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature									
Unauthorised downloading or uploading of files or use of file sharing.									
Using proxy sites or other means to subvert the school's filtering system.									

Accidentally accessing offensive or pornographic material and failing to report the incident.									
Deliberately accessing or trying to access offensive or pornographic material.									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.									
Unauthorised use of digital devices (including taking images)									
Unauthorised use of online services									
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.									

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a 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				
Deliberate actions to breach data protection or network security rules.								
Deliberately accessing or trying to access offensive or pornographic material								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Using proxy sites or other means to subvert the school's filtering system.								
Unauthorised downloading or uploading of files or file sharing								
Breaching copyright or licensing regulations.								
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.								
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers								
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail								
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.								
Failing to report incidents whether caused by deliberate or accidental actions								
Continued infringements of the above, following previous warnings or sanctions.								

Online Safety Education Programme

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

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'."*

Keeping Children Safe in Education states:

> *"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"*

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways (statements may need to be adapted, depending on school structure and the age of the learners).

- A planned online safety curriculum for all year groups matched against a nationally agreed framework e.g. Education for a Connected Work Framework by UKCIS/DCMS and the SWGfL Project Evolve and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.

- 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. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990. Lessons and further resources are available on the Cyber-Choices site.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, 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 should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Learners

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

- mechanisms to canvass learner feedback and opinion.
- appointment of digital leaders/anti-bullying ambassadors/peer mentors (or similar groups)
- the Online Safety Group has learner representation
- learners contribute to the online safety education programme e.g. peer education, digital leaders leading lessons for younger learners, online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

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

> "All staff should receive appropriate safeguarding and child protection training (**including online safety**) at induction. The training should be **regularly updated**. In addition, all staff should receive safeguarding and child protection (**including online safety**) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, **including online safety** training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows: (select/delete as appropriate)

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events, (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required

Governors

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

- attendance at training provided by the local authority/MAT or other relevant organisation (e.g., SWGfL)
- participation in school training / information sessions for staff or parents (this may include attendance at assemblies/lessons).

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

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will seek to provide information and awareness to parents and carers through:

- *regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes*
- *regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carer evenings etc*
- *the learners – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by learners leading sessions at parent/carer evenings.*
- *letters, newsletters, website, learning platform,*
- *high profile events / campaigns e.g. Safer Internet Day*
- *reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).*
- *Sharing good practice with other schools in clusters and or the local authority*

Adults and Agencies

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

- online safety messages targeted towards families and relatives.
- providing family learning courses in use of digital technologies and online safety
- providing online safety information via their website and social media for the wider community
- supporting community groups, e.g. early years settings, childminders, youth/sports/voluntary groups to enhance their online safety provision (consider supporting these groups with an online safety review using 360 Groups or 360 Early Years).

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection. (Schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational, and administrative staff before these statements are agreed and added to the policy).

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

> "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…
> The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

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

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead

responsibility for safeguarding and online safety and the IT service provider will have technical responsibility. T**he filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider.**

- **checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when** a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced **e.g. using SWGfL Test Filtering**

Filtering

- *the school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.*
- *illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated*
- *there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective*
- *there is a clear process in place to deal with, and log, requests/approvals for filtering changes (see Appendix for more details).*
- *filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.*
- *the school has (if possible) provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)*
- *younger learners will use child friendly/age-appropriate search engines e.g. SWGfL Swiggle*
- *the school has a mobile phone policy and where personal mobile devices have internet access through the school network, content is managed in ways that are consistent with school policy and practice.*
- *access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.*

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

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

- *The school monitors all network use across all its devices and services*
- *monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored*
- *There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention*
- ***Management of serious safeguarding alerts is consistent with safeguarding policy and practice***

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

- *physical monitoring (adult supervision in the classroom)*
- *internet use is logged, regularly monitored and reviewed*
- *filtering logs are regularly analysed and breaches are reported to senior leaders*
- *pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.*
- *where possible, school technical staff regularly monitor and record the activity of users on the school technical systems*
- *use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)*

Technical Security

The 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):

- *responsibility for technical security resides with SLT who may delegate activities to identified roles*
- *all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT/Online Safety Group*
- *password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)*
- *the security of their username and password and must not allow other users to access the systems using their log on details.*

- *all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.*
- *all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.*
- *the administrator passwords for school systems are kept in a secure place, e.g. school safe*
- *there is a risk-based approach to the allocation of learner usernames and passwords*
- *there will be regular reviews and audits of the safety and security of school technical systems*
- *servers, wireless systems and cabling are securely located and physical access restricted*
- *appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software*
- *there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,*
- *(insert name or role) is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied*
- *an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)*
- *use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them*
- *personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network*
- *staff members are not permitted to install software on a school-owned device without the consent of the SLT/IT service provider*
- *removable media is not permitted unless approved by the SLT/IT service provider*
- *systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)*
- *mobile device security and management procedures are in place (where mobile devices are allowed access to school systems). (Schools may wish to add details of the mobile device security procedures that are in use).*
- *guest users are provided with appropriate access to school systems based on an identified risk profile*

Mobile Technologies

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

> *"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.*

Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage.

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

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 strategies is possible. However, these need to be thoroughly researched, risk assessed and aligned with existing policy prior to implementation. A more detailed mobile technologies policy template can be found in the Appendix.

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

The school allows:

	School devices			Personal devices		
	School owned for individual use	School owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	No	Yes	No	No	Yes	Yes
No network access				Yes	Yes	Yes

Aspects that the school may wish to consider and include in their Online Safety Policy, mobile technologies policy or acceptable use agreements may include the following:

School owned/provided devices:

- *all school devices are managed though the use of Mobile Device Management software*
- *there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed*
- *any designated mobile-free zone is clearly signposted*
- *personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated*
- *the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.*
- *liability for damage aligns with current school policy for the replacement of equipment*
- *education is in place to support responsible use*

Personal Devices:

- *there is a clear policy covering the use of personal mobile devices on school premises for all users*
- *where devices are used to support learning, staff have been trained in their planning, use and implementation, ensuring that all learners can access a required resource*

[3] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- *where personal devices are brought to school, but their use is not permitted, appropriate, safe and secure storage should be made available. (this needs to be shaped according to current mobile phone school policy)*
- *use of personal devices for school business is defined in the acceptable use policy and staff handbook. Personal devices commissioned onto the school network are segregated effectively from school-owned systems*
- *the expectations for taking/storing/using images/video aligns with the school's acceptable use policy and use of images/video policy. The non-consensual taking/using of images of others is not permitted.*
- *liability for loss/damage or malfunction of personal devices is clearly defined*
- *there is clear advice and guidance at the point of entry for visitors to acknowledge school requirements*
- *education about the safe and responsible use of mobile devices is included in the school online safety education programmes*

Social Media

With widespread use 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 learners, the school and the individual when publishing any material online.

Expectations for teachers' professional conduct are set out in the DfE Teachers Standards but all adults working with children and young people must understand that the nature and responsibilities of their work place them in a position of trust and that their conduct should reflect this.

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school 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 learners through:

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

School staff should ensure that:

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

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

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

Personal Use

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

Monitoring of Public Social Media

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

- *when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure*

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

The social media policy template in Appendix C4 provides more detailed guidance on the school's responsibilities and on good practice.

Digital and video images

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

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

- *the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance/policies. Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education*
- *when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images*
- *staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes*
- *in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on*

social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images

- *staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images*
- *care should be taken when sharing digital/video images that learners are appropriately dressed*
- *learners must not take, use, share, publish or distribute images of others without their permission*
- *photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy*
- *learners' full names will not be used anywhere on a website or blog, particularly in association with photographs*
- *written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. (see parents and carers acceptable use agreement in the Appendix). Permission is not required for images taken solely for internal purposes*
- *parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy*
- *images will be securely stored in line with the school retention policy*
- *learners' work can only be published with the permission of the learner and parents/carers*

Online Publishing

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

- *Public-facing website*
- *Social media - limited*
- *Online newsletters*
- *Other (to be described)*

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

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

The school public online publishing provides information about online safety e.g., publishing the schools Online Safety Policy and acceptable use agreements; curating

latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Data Protection

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

- has a Data Protection Policy which is reviewed every 2 years or if necessary due to updates or changes in legislation (model policy framework adopted from the LA)
- implements the data protection principles and can demonstrate that it does so
- has paid the appropriate fee to the Information Commissioner's Office (ICO)
- *has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest.*
- *has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it*
- *the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed*
- *has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it*
- *information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed*
- *will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this*
- *data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals*
- *provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)*

- *has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them*
- *carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier*
- *has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors*
- *understands how to share data lawfully and safely with other relevant data controllers.*
- *has clear and understood policies and routines for the deletion and disposal of data*
- *reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents*
- *has a Freedom of Information Policy which sets out how it will deal with FOI requests*
- *provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff*

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

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

Staff must ensure that they:

- *at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse*
- *can recognise a possible breach, understand the need for urgency and know who to report it to within the school*

- *can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school*
- *only use encrypted data storage for personal data*
- *will not transfer any school personal data to personal devices. Procedures are in place to enable staff to work from home (i.e. VPN access to the school network, or a work laptop provided).*
- *use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data*
- *transfer data using encryption, a secure email account (where appropriate), and secure password protected devices*

The Personal Data Advice and Guidance in the appendix (C2) provides more detailed information on the school's responsibilities and on good practice.

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- *there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training*
- *there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors*
- *parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising*
- *online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate*
- *the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy*

Appendices

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the SWGfL website. The appendices are as follows:

A1 - Learner Acceptable Use Agreement Template – for older learners
A2 - Learner Acceptable Use Agreement Template – KS2
A3 - Learner Acceptable Use Agreement Template – for younger learners (Foundation/KS1)
A4 - Parent/Carer Acceptable Use Agreement Template
A5 - Staff (and Volunteer) Acceptable Use Policy Agreement Template
A6 - Community Users Acceptable Use Agreement Template
A7 – Online Safety Group Terms of Reference Template
A8 - Harmful Sexual Behaviour Policy Template (new template added September 2022)
A9 - Computer Misuse and Cyber Choices Policy Template
A10 - Responding to incidents of misuse – flow chart
A11 - Record of reviewing devices/internet sites (responding to incidents of misuse)
A12 - Reporting Log
B1 - Training Needs Audit Log
C1 - Technical Security Policy Template (including filtering and passwords)
C2 - Personal Data Advice and Guidance
C3 - School Online Safety Policy Template: Electronic Devices - Searching Screening and Confiscation (new DfE guidance from September 2022)
C4 - Mobile Technologies Policy Template (inc. BYOD/BYOT)
C5 - Social Media Policy Template

Legislation
Links to other organisations and resources
Glossary of Terms

The Bradshaw Hall Primary School would like to acknowledge the use of this template as advised by Stockport MBC Local Authority Safeguarding Partnership, November 2024

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 2024**
Date Ratified & Adopted by the Governing Board:	**Autumn 2024**
Signed - Head Teacher	
Signed - Chair of Governing Board	
Next Review:	**Autumn 2025**
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. All staff and volunteers will act in accordance with this and all relevant codes of conduct and professionalism associated with safeguarding children in accordance with the current Keeping Children Safe in Education legislation.
Failure to adhere to established professional codes of conduct will result in serious misconduct proceedings being invoked.

I understand a copy 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: