PALFREY INFANT SCHOOL
ONLINE SAFETY POLICY
Lead Teacher: A Hennefer

Reviewed and amended: September 2025
As a Rights Respecting School we believe:
Every child has to learn and have an education. Article 28 & 29
Every child has a right to be safe from harm and abuse. Article 19
Every child has a right of freedom of expression. Article 13
Every child has a right to be part of a community and practise his or her own religion and use his or her own language. Article 30
Every child has a right to rest and leisure. Article 31
Every child has a right to keep healthy. Article 24

We believe we fulfil these rights at Palfrey Infant School

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body / Governors Sub Committee on:	September 2025
The implementation of this Online Safety policy will be monitored by the:	*Alison Walsh - Head teacher* *Anna Hennefer – Deputy Head and Online Safety Coordinator*
Monitoring will take place at regular intervals:	1 year later
The Governing Body / Governors Sub Committee will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	1 year later
The Online 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 online safety or incidents that have taken place. The next anticipated review date will be:	1 year later
Should serious online safety incidents take place, the following external persons / agencies should be informed:	MASH, Police, LADO, Early Help leads

Scope of the Policy

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

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

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school. This Policy document has been drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements both in school and at home. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in Education September 2025 states 'As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material…support governing bodies and proprietors keep their children safe online (including when they are online at home)'

Governors*:*

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents, monitoring reports. Governors should attend annual training relating to online safety. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- reporting to relevant Governors
- Review the risk profile of the school and ensure that the filtering and monitoring solutions meet the needs of this risk profile

Headteacher* and *Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Co-ordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher/ Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team / Senior Management Team will receive regular monitoring reports.

- The headteacher will remain responsible for the filtering and monitoring solutions in order to protect users from seeing inappropriate content and behaving appropriately whilst on devices.

***Online Safety* Coordinators*:* (Anna Hennefer)**

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- meets regularly with Online Safety Governor to discuss current issues
- attends relevant meeting / committee of Governors
- reports regularly to Senior Leadership Team

Network Manager / Technical staff*:*

The Network Manager / Technical Staff / is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network / internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher/ Senior Leader*;* Online Safety Coordinator for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. Visiting teachers use generic log in for teachers.
- School buy into a service level agreement with LA ICT support team, the school are responsible for ensuring that these activities take place and direct their ICT technician to complete these activities.

Teaching and Support Staff:

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Head teacher/ Senior Leader; Online Safety Coordinator for investigation / action / sanction

- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they actively monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use will be pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Work devices are to be used for professional responsible use. Not by members of family or for anything other than work related tasks.

Designated Safeguarding Leads (DSL's) and Deputy DSL's: (Alison Walsh, Anna Hennefer, Tina Dunkley and Mary Adams)

Should be trained in Online 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
- online-bullying

Pupils:

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

Parents / Carers:

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

- digital and video images taken at school events

Education – Pupils

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

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

- A planned online safety lesson should be provided as part of Computing / PHSE / other lessons and should be regularly visit (once every ½ term) using Project Evolve to identify the areas of teaching and support pupils need
- Key online safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- In lessons, internet use will be pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet whilst being taught how to use a search engine, staff should be vigilant in monitoring the content of the websites the young people visit.
- Pupils should be taught about dis and misinformation alongside conspiracy theories as part of the curriculum in the relationships education.

Education – Parents / Carers

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

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

- Curriculum activities
- Letters, newsletters,
- Parents / Carers evenings / workshops (Walsall Street Teams/ NSPCC)
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

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

- **A planned programme of formal online safety training will be made available to staff and governors. This will be updated annually and reinforced.**
- **All new staff should 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 is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on school devices. Staff who wish to use memory sticks must hand them in for encryption by Wolverhampton E-services Schools Technology Support. **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**

Training – Governors

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

- Attendance at training provided by the Local Authority
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by ICT Co-ordinator. Users are responsible for the security of their username and password termly.
- The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader and kept in a secure place (e.g. school safe)
- Computing Co-ordinator is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users using Fortinet software. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored by using https://testfiltering.com. This is monitored every half term by A Hennefer logging into different devices as different users and saving the results to the school network should anyone

request to see these. There is a clear process in place to deal with requests for filtering changes.

- The school has provided enhanced / differentiated user-level filtering for different access between pupils and staff
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed on CPOMS.
- School technical staff should regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. They should be given differentiated log ins and not use someone else's.
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
- **Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured**.

Smoothwall Monitor is used across the network in order to

- Monitor inappropriate use of language
- Monitor internet usage Inc. words associated with the prevent agenda
- Enforce the agreement of the Acceptable Use Policy (See Appendix)

Any identified incident is reported to Alison Walsh and Anna Hennefer in order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by a Local authority online safety advisor and reported via email.
A weekly report that is a reassurance email that gives an update on the number of users (people who log into devices), the number of devices that are being monitored and number of captures in the week. A monthly report is sent that includes details relating to school captures and incidents. This helps and supports us to identify the risk profile and look at patterns in the captures.

The monitoring software does not negate the need for staff to supervise pupils when using devices and it should be noted that it works on networked devices and Chromebook but not iPads. iPad use should be fully supervised by staff and websites given to pupils in order to reduce the risk of coming across inappropriate content, using Swiggle.org.uk as a search engine to add an additional level of filtering.

Managing filtering

The school work with ICT support technicians from LA ICT to ensure systems to protect pupils are reviewed on at least an annual basis. The software used for the filtering solution is Fortinet. If staff come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator and or DSL. Staff have a responsibility to also inform the school's IT support at LA ICT. If pupils come across unsuitable on-line materials, the site must be reported to their teacher who will inform the Online Safety Coordinator. Staff are now able to access sites such as 'You Tube' and others on request but staff need to be aware that these sites do contain inappropriate materials and therefore children are not allowed to use these sites. Links and content should be shared and checked in school by staff just prior to use in the classroom due to daily rotation of advertising content.

The filtering system is checked at least half termly on different devices and logins by the online safety coordinator, using www.testfiltering.com. This test will be carried out whilst on the school premises and the outcomes will be recorded on admindocs (saved) for reference.

Communications

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

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

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

- **The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
- **Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.**
- **Any digital communication between staff and pupils or parents / carers (email, text messages etc.) must be professional in tone and content.** These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used.

- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

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

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school 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

Internet-enabled mobile phones and devices

More and more people have access to sophisticated new internet-enabled devices such as mobile phones, tablets and games consoles.

It is important that whilst the school recognises the potential advantages these devices can offer, there are clear and enforceable rules for their use in school, particularly when they give access to the Internet, and allow pictures and information to be remotely posted to a website or blog.

Pupils will be taught the legal and moral implications of posting photos and personal information from mobile phones to public websites etc. and how the data protection and privacy laws apply.

Pupils are not allowed to have personal mobile phones or other similar devices in school. Parents may request that such devices are kept at the School Office for pupils who may need them on their journey to and from school.

Staff personal devices, including mobile phones and smart watches should be turned off and locked away during learning time and not used in the vicinity of children whilst in designated areas of the school.

Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.
The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:
• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
• **contact:** being subjected to harmful online interaction with other users; for example: child on child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
• **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.
And include Dis and misinformation, as well as conspiracy theories

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

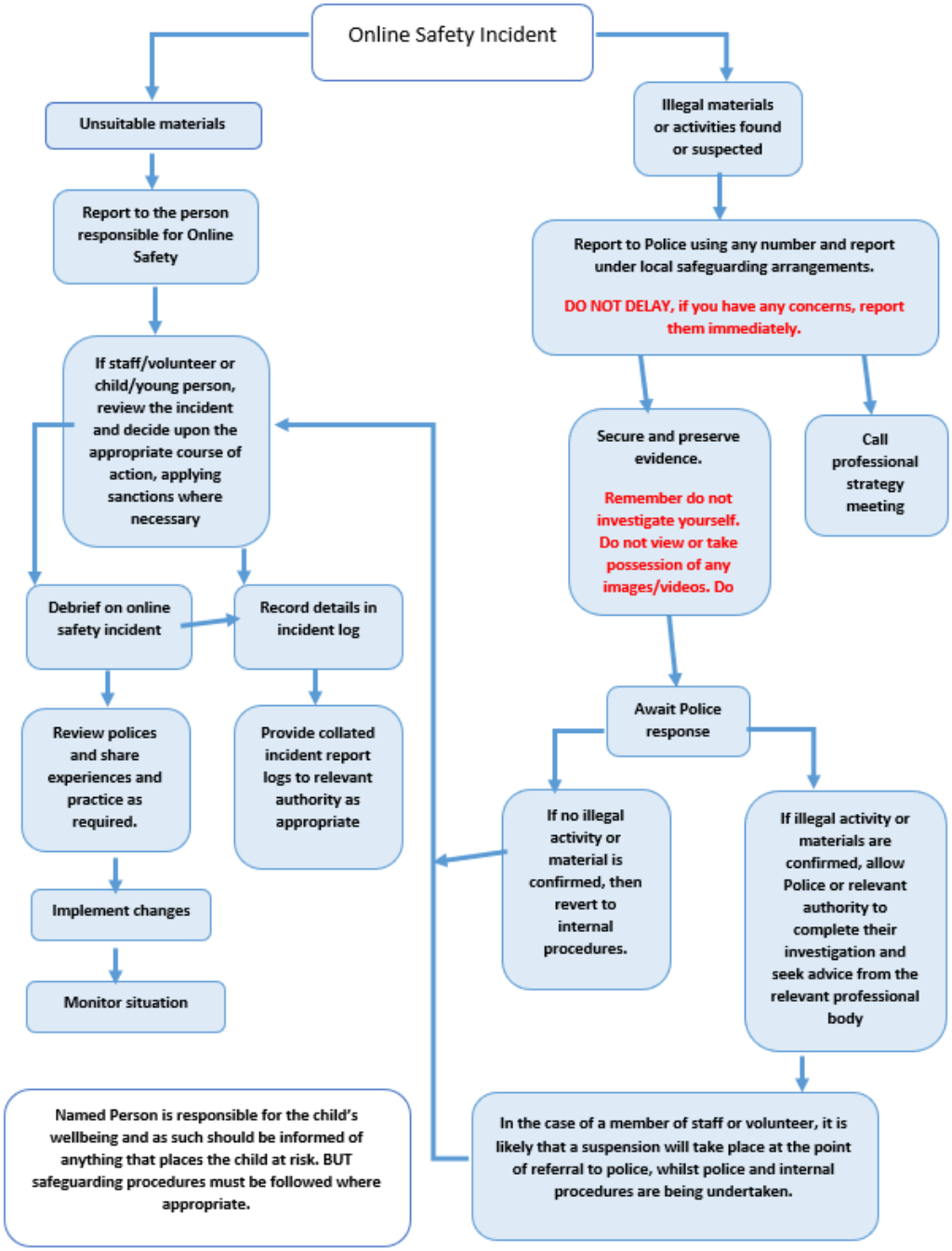
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		x				
On-line gaming (non-educational)			x			
On-line gambling					x	
On-line shopping / commerce					x	
File sharing					x	
Use of social media					x	
Use of messaging apps					x	
Use of video broadcasting e.g. You tube (for lessons by teachers)		x				
Use of video broadcasting e.g. You tube (children and non-educational)					x	

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above)

Illegal Incidents

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



Other Incidents

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

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

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

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

School Actions & Sanctions

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

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

Using proxy sites or other means to subvert the school's filtering system	x	x	x	x	x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x	x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x	x	x	x	x	x	x	x	x

Actions / Sanctions

Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	x	x	x	x	x	x	x	x
Inappropriate personal use of the internet / social media / personal email	x	x	x	x	x	x	x	x
Unauthorised downloading or uploading of files	x	x	x	x	x	x	x	x
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	x	x	x	x	x	x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x	x	x	x	x	x
Deliberate actions to breach data protection or network security rules	x	x	x	x	x	x	x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	x	x	x	x	x	x	x	x
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	x	x	x	x	x	x	x	x
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils	x	x	x	x	x	x	x	x

Actions which could compromise the staff member's professional standing	x	x	x	x	x	x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x	x	x	x	x	x	x	x
Using proxy sites or other means to subvert the school's / academy's filtering system	x	x	x	x	x	x	x	x
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x	x	x	x	x	x	x
Deliberately accessing or trying to access offensive or pornographic material	x	x	x	x	x	x	x	x
Breaching copyright or licensing regulations	x	x	x	x	x	x	x	x
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x	x

Acceptable Use Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.
- No one enters into any personal transaction that involves the school or a school device
- Visit sites that might be defamatory or incur liability on the part of the school or adversely impact on the image of the school
- Upload, download, or otherwise transmit (make, produce or distribute) commercial software or any copyrighted materials without written permission
- Reveal or publicise confidential or proprietary information, which includes, but is not limited to: financial information, personal information, databases and the information contained therein, computer/network access codes, and business relationships
- Intentionally interfere with the normal operation of the Internet connection, including the propagation of computer viruses and sustained high volume network traffic (sending or receiving of large files or sending and receiving of large numbers of small files or any activity that causes network congestion) that substantially hinders others in their use of the Internet
- Use the Internet for soliciting, representing personal opinions or revealing confidential information or in any other way that could reasonably be considered inappropriate
- Gambling, or any gaming involving possible financial gain or loss.

Acceptable Use Policy for learners in Early Years and KS1

Learners will read and sign the acceptable use policies outlined on Purple Mash and the school internet rules.

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in Education states 'As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material…support governing bodies and proprietors keep their children safe online (including when they are online at home)'

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign to show their support of the school in this important aspect of the school's work.

Palfrey Infant School
Bescot Street
Walsall
WS1 4HY

Telephone: 01922 720713
Fax: 01922 720104
E-mail: postbox@palfreyinfant.co.uk **Headteacher: Mrs A Walsh**

DATE: 18.9.2023

Dear Parents,

Acceptable Use of the Internet

As part of pupils' curriculum enhancement and the development of computing skills, Palfrey Infant School is providing supervised access to the Internet, including E-mail.

Although there are concerns about children having access to undesirable materials, we are taking positive steps to deal with this risk in school. Walsall Council operates a filtering system that restricts access to inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the Council or School cannot be held responsible for the nature and content of materials accessed through the Internet.

Children will be given lessons on the safe use of the Internet to help lessen any risks to their safety. We will also be using Swiggle.org.uk as a child-friendly internet search engine to add an additional level of filtering. For more information and to use this search engine at home, visit https://swgfl.org.uk/services/swiggle/

I enclose a copy of the Acceptable Use Policy for the Internet and E-mail, which is age appropriate for your child. Please read it and share with your child at home to ensure your child has safe access to the Internet and e-mail facilities to enhance their learning, both at home and at school.

Yours sincerely

Headteacher
A Walsh

Acceptable Use Agreement (KS1)

I will treat the mobile devices and computers with respect.

I will only use the internet when an adult has allowed me to and I will only use programmes and websites that I have been told to use.

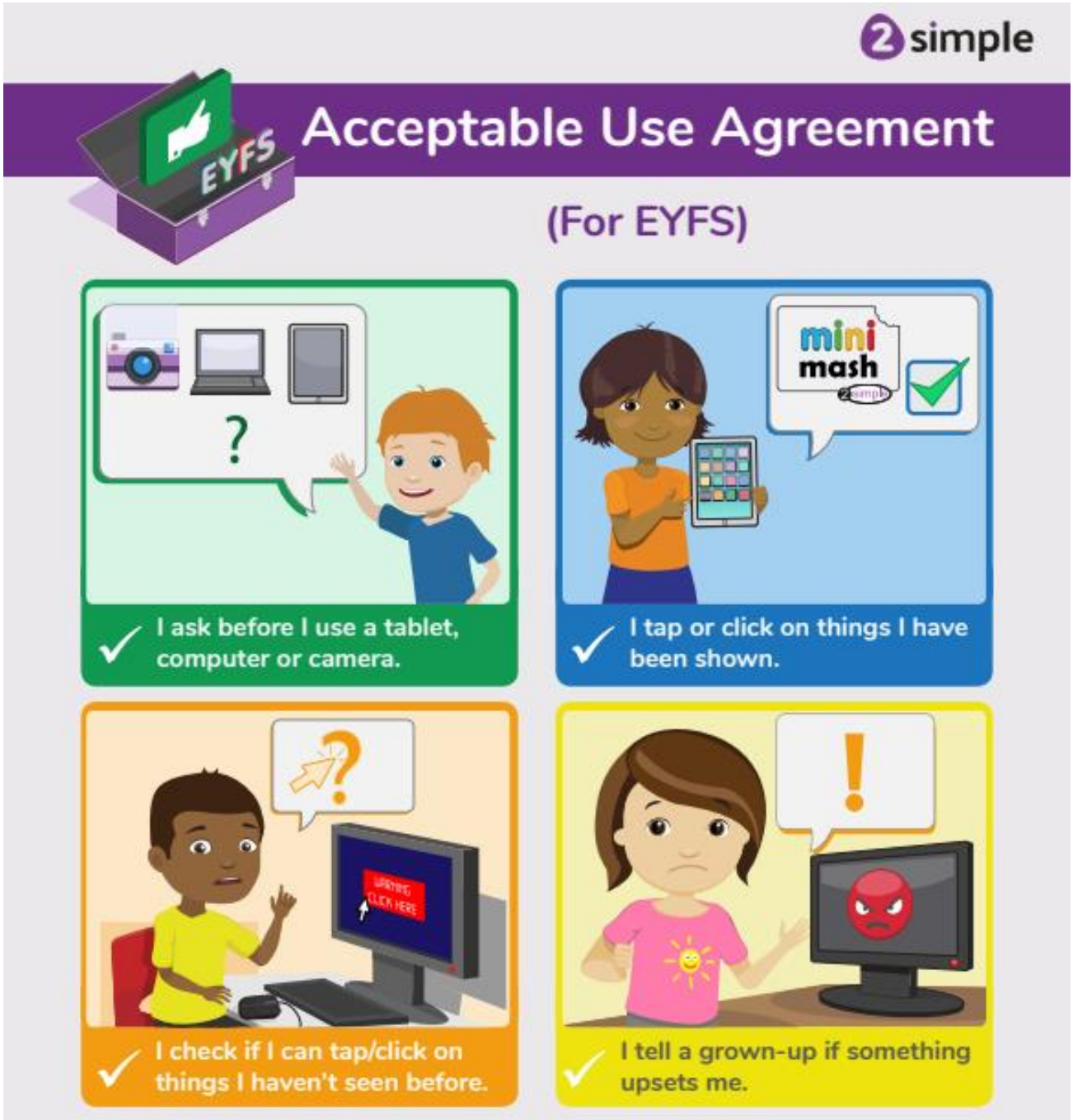
I promise to click on the Swiggle hand and then tell a teacher if there is a problem.

I will always keep my personal information to myself, including my login name and password.

I will always tell an adult if I see something on a screen that upsets me, or I am unsure of.

I will only send messages that are polite and sensible with support from a teacher and I will not communicate online with people I don't know in the real world.

I will not eat or drink near any school computers.


2simple
EYFS
Acceptable Use Agreement
(For EYFS)
I ask before I use a tablet, computer or camera.
mini mash
I tap or click on things I have been shown.
I check if I can tap/click on things I haven't seen before.
I tell a grown-up if something upsets me.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times. It is the duty of the school to ensure that every child in our care is safe, and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical buildings. Keeping Children safe in states 'As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material…support governing bodies and proprietors keep their children safe online (including when they are online at home)'

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will not use the systems for personal or recreational use within the policies and rules set down by the school due to the cybersecurity risks.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will set strong passwords (a strong password is one which uses a combination of letters, numbers and other permitted signs)
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school Computing systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices, smart watches etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....