Chuckery Primary School

Chuckery
Primary School

Working Together

Online Safety Policy & Acceptable User Agreement

Completed By:	Angella McMorrow
Date Completed:	September 2024
Agreed by Governors:	September 2024
To be reviewed:	September 2027

Introduction

Chuckery Primary School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment. Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at Chuckery Primary School we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Online Safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for Chuckery Primary School.

Our Online Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors.

- The school's Online Safety co-ordinator is Ms McMorrow alongside Ms A Cuthill computing leader and deputy online safety co-ordinator and the computing technician Mr Riley
- The Online Safety Governor is Mrs Nicola Rudge
- The Online Safety Policy and its implementation shall be reviewed annually.
- It is approved by the Governors and will be reviewed annually
- It is to be used/read in conjunction with our other Safeguarding Policies:
    - Acceptable use of Data & computing Policy
    - Anti-Bullying Policy
    - Behaviour Policy
    - Child Protection Policy
    - GDPR Policies
    - Photographing Children & Adults Policy
    - Social Networking Policy
    - Code of Conduct

Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. The role of the Online Safety Governor will include:

- Regular meetings with the Online Safety Co-ordinator/computing Technician
- Regular monitoring of Online Safety incident logs.
- Attendance at relevant training in order to maintain safeguarding awareness on an annual basis

Head teacher and Senior Leaders:

- The Head teacher/SLT are responsible 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 Coordinator/computing Technician.
- The Head teacher/SLT are responsible for ensuring that the Online Safety Coordinator/computing Technician and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head teacher/SLT 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 Head teacher/SLT should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made.

The Online Safety Co-ordinator:
Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policy/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 school computing technical staff.
- Receives reports of Online Safety incidents and creates a log of incidents to inform future online safety developments.

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 skills and understanding are embedded in all aspects of the curriculum and other activities including through the pre-planned Online safety curriculum using Project Evolve
- 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 internet use should be pre-planned and 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

Designated Safeguarding Lead

Is 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, website 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
- access to Online safety sections of the website
- their children's personal devices in the school (where this is allowed)

Teaching and Learning

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access is differentiated for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not in online safety and cross curricular lessons.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation through the computing curriculum, these skills should be practiced and used, in those year groups in a cross curricular manner too as planned into the mini adventure curriculum.
- As part of the new curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, digital footprints and online bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through computing we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society. We also measure and assess the impact regularly through SLT & Governor meetings and also with individual teachers to ensure all children have equal access to succeeding in this subject. Pupils are to be taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.

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 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 is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are being taught how to use a search engine and are allowed to search the internet, staff should discuss the key words needed in the search engine with pupils, using a verified filtered search engine e.g. Swiggle/Kiddle, have looked up searches prior to the lesson and be vigilant in monitoring the content of the websites the young people visit.

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. This will be regularly updated 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.
- The Online Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (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 Online Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors / Directors

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 / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff or parents

Authorised Internet Access

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to Online Safety and agree to its use:

- All staff must read and sign the 'Acceptable computing User Agreement' before using any school computing resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Head teacher, by recording the incident in CPOMS.
CPOMS will be reviewed regularly by the Online Safety Co-ordinator.
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible using Netsweeper.

The school uses Smoothwall monitor who provides the school with the most comprehensive Online Safety solution for monitoring to keep users safe online while allowing them access to all of the benefits of the online world.

Using Smoothwall protects students by monitoring, capturing and alerting us to potentially harmful content or behaviour allowing us to safeguard against online dangers such as inadvertent exposure to inappropriate websites, online-bullying, grooming, online gambling and un-moderated chatrooms.

Communication

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 (e.g. by remote access). Not for personal communications.
- 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, social media, chat, blogs, 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.
- 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.

	Staff & other adults			Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with headteachers 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 (staff room)	x							x
Taking photos on mobile phones / cameras				x				x
Use of other mobile devices e.g. tablets, gaming devices				x				x
Use of personal email addresses in school , or on school network				x				x
Use of school email for personal emails				x				x
Use of messaging apps				x				x
Use of social media				x				x
Use of blogs				x				x

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 Mr Owen Riley who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term. Year 5 and 6 have the capability to change their own passwords and the rest of the school have individual logins with one password to remember.

- 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)

- Mr Owen Riley are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced / differentiated user-level filtering School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed.
- 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. These guest logins are managed by Mr Owen Riley and are given out for temporary access and then removed at the end of the period of working in school.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school, Staff are not allowed to access certain websites at home and family member access is strictly denied.
- An agreed policy is in place that allows staff forbids staff from downloading executable files and installing programmes on school devices. Mr Owen Riley are the people who are in charge of downloading and installing programmes so staff should seek advice from them prior to doing this.

- No personal equipment (e.g. memory sticks / CDs / DVDs) should be connected to or used with the School's ICT systems ('GDPR Staff Acceptable Use and Policy and Agreement pg 2). Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Personal data should not be stored on removable devices e.g. children's photographs, names and any reference to children.
    - Staff should use the VPN to access personal information about pupils rather than using removable storage

Monitoring
The school will monitor and enforce the policy through: e.g.

- Smoothwall monitor Monitoring- provides the most advance monitoring that is moderated by vast AI technology and human specialists. Schools are alerted immediately should an incident arise. Smoothwall monitor is the only solution of its kind that continuously builds a profile of all users, allowing the system to accurately interpret between a one-off event as well as a consistent pattern of behaviour.
- Teacher planning
- Log of any incidents: Will be dealt with by Lisa Francis, Gavin Dwyer, Sally Hanson
- Online safety survey for children –
- Online safety team at Walsall Education
- Technical Staff as part of SLA agreement with Walsall Council ICT services to ensure all security software, including virus software and settings are kept up to date

Every member of the school community has a duty of care to online safety as part of safeguarding. This policy deals with incidents associated with the use of technology that affects our school community.

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. Incidents that occur outside of school are covered by parent's duty of care.

Monitoring solution

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 Angela McMorrow, Owen Riley, Amy Cuthill and the safeguarding team via CPOMs in order for it to be investigated and dealt with. Incidents of every level are also monitored and reported by the 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 viewed 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 chromebooks 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.

Managing filtering

The school will work with Walsall School ICT support to ensure systems to protect pupils are reviewed. If staff comes across unsuitable on-line materials, the site must be reported immediately to the online safety Coordinator. 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 checked in school just prior to use in the classroom due to daily rotation of advertising content and ability to access in school.**

Owen Riley will ensure that the school's filtering system is working by randomly checking logins and devices, half termly, using 'test filtering' www.testfiltering.com. A screen shot of the checks will be made and saved on the school's network.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff should be encouraged to change passwords regularly and can use a password manager as necessary to avoid password duplication.

Staff must always 'lock' the PC if they are going to leave it unattended.

Social Networking

Please see our separate Social Networking Policy

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

User Actions		Acceptable	Acceptableatcertaintimes	Acceptablefornominatedusers	Unacceptable	Unacceptableandillegal
UsersshallnotvisitInternetsites,make,post,download, upload,datatransfer,communicateorpasson,material, remarks,proposalsorcommentsthatcontainorrelateto:	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.					
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					
	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					
	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 (eg 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				

X

X

X

On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce				x	
File sharing				x	
Use of social media			x		
Use of messaging apps				x	
Use of video broadcasting e.g. Youtube			x		

Reporting

All breaches of the Online Safety policy need to be recorded on CPOM's using the Online Safety category, this is then reported to the appropriate staff members. The details of the user, date and incident should be reported. Incidents which may lead to child protection issues need to be passed on to the Head teacher / SLT immediately - it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require SLT intervention (e.g. online bullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the Head teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

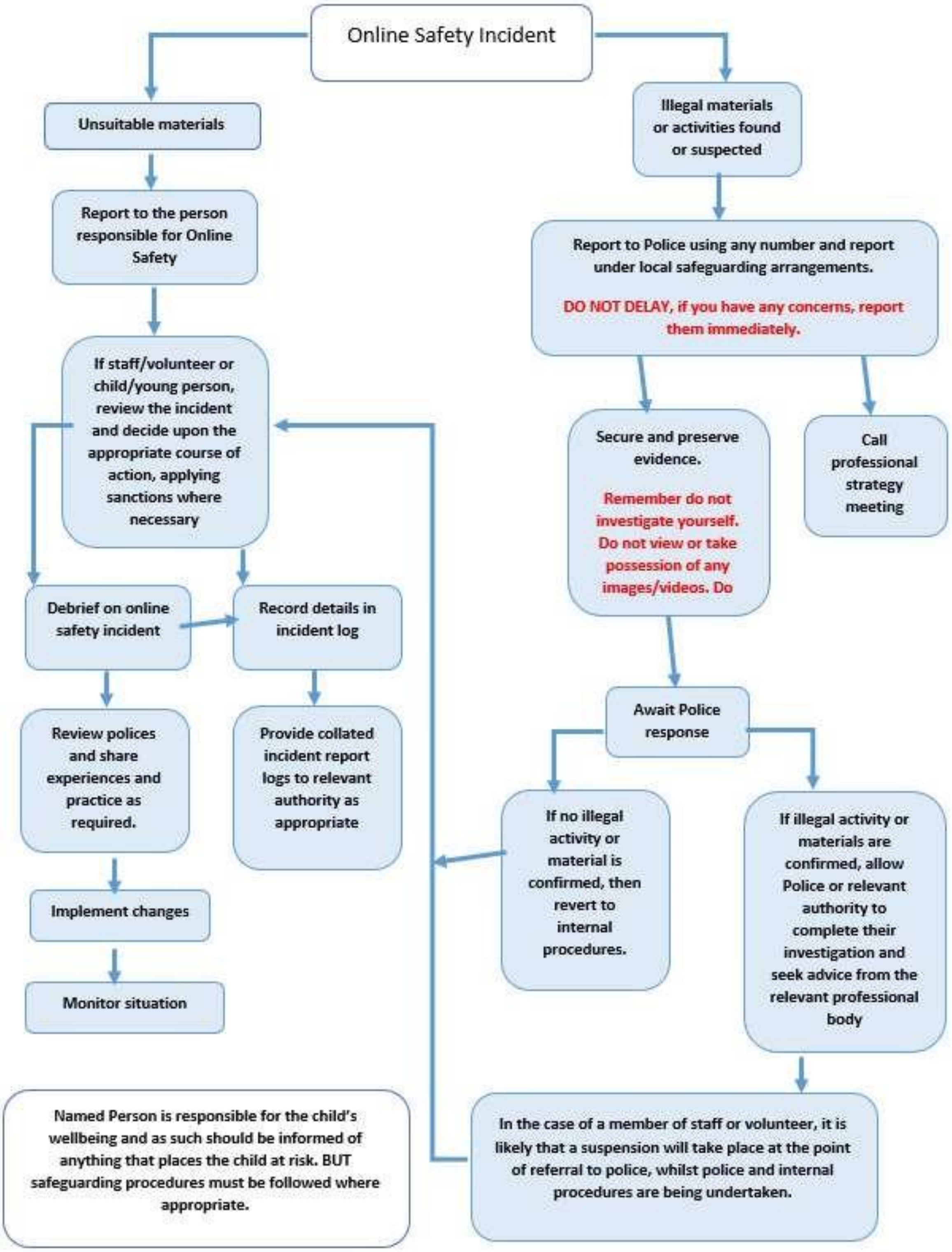
Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, Childline)

Handling Online Safety Complaints/Incidents

- Complaints of Internet misuse will be dealt with by the Head teacher.
- Any complaint about staff misuse must be referred to the Head teacher.
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
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.

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: o Internal response or discipline procedures o Involvement by Local Authority / Academy Group or national / local organisation (as relevant). o 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:

  o incidents of 'grooming' behaviour o the sending of obscene materials to a child

  o adult material which potentially breaches the Obscene Publications Act o criminally racist material o promotion of terrorism or extremism o 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 /	Refer to Headteacher /	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet	Warning	Further sanction eg detention /
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).									
Unauthorised use of non-educational sites during lessons					x				
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device									
Unauthorised / inappropriate use of social media / messaging apps / personal email					x				
Unauthorised downloading or uploading of files					x				

Allowing others to access school network by sharing username and passwords					x				
Attempting to access or accessing the school network, using another student's / pupil's account					x				
Attempting to access or accessing the school network, using the account of a member of staff					x				
Corrupting or destroying the data of other users					x				
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature					x				
Continued infringements of the above, following previous warnings or sanctions					x				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school					x				
Using proxy sites or other means to subvert the school's filtering system					x				
Accidentally accessing offensive or pornographic material and failing to report the incident					x				
Deliberately accessing or trying to access offensive or pornographic material					x				
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act					x				

	Actions / Sanctions							
Staff Incidents	Refertolinemanagerr	RefertoExecutive Head teacherPrin	RefertoLocalAuthority/HR	RefertoPolice	RefertoTechnicalSupport Staffforactionrefilteringetc.	Warning	Suspension	Disciplinaryaction
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
Inappropriate personal use of the internet / social media / personal email	x	x	x					
Unauthorised downloading or uploading of files	x	x						
Allowing others to access school network by sharing username and passwords or attempting to access or		x	x		x			x

accessing the school network, using another person’s account								
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	x	x		x	x	x	x
Deliberate actions to breach data protection or network security rules	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
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	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
Actions which could compromise the staff member’s professional standing	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
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
Continued infringements of the above, following previous warnings or sanctions	x	x	x	x	x	x	x	x

Mobile Devices

Many new mobile devices can have access to the Internet. There are risks of mobile bullying, or inappropriate contact.

- Pupils by permission of the Head teacher can bring mobile devices onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into the school office at the start of the day and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should always use the school phone to contact parents.
- All staff, visitors and volunteers should ensure that their phones are turned off and stored safely away during the teaching day unless given express permission from Executive Head teacher.
- Staff may use their mobile phones in the staffroom/one of the school offices during break/lunch time.
- Caretaker and Catering staff are issued with a mobile phone for the purpose of their role. The phone provided does not have an internet or photo capability - the phone is solely to be used for making and receiving work related calls.
- Parents cannot use mobile phones in/around school or on school trips to take photographs of the children - please see Photographing Children and Adults Policy.
- On trips/offsite visits/swimming staff are provided with mobiles that can be used for emergency only - these do not have internet or photo capability.

Digital/Video Cameras/Photographs
Please see our separate Photographing Children & Adults Policy & Social Networking Policy

Published Content and the School Website
The school website is a valuable source of information for parents and potential parents.

Contact details on the Website will be the school address, e-mail and telephone number.

- Staff and pupils' personal information will not be published.
- The Head teacher or computing Technician/Online Safety Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.

 Work will only be published with the permission of the pupil and parent. 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 pupils in the digital / video images.

- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School computing systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- Online Safety will be discussed with our computing support and those arrangements incorporated in to our agreement with them.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the GDPR Policies.

Assessing Risk
The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit computing use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate.

Communication of Policy
Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during computing lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School Online Safety Policy and its importance explained.

Parents:

- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school Website.

Link to behaviour policy -

- 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 cyber-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.

Policy Review

The policy was last reviewed and agreed by the Governing Body on 13th May 2020. It is due for review Sept 2021.

Signed:	Signed:
	N. Rudge
Print: Mr. James Pearce	Print: Mrs. Nicola Rudge
Date: 22nd January 2024	Date: 22nd January 2024
Executive Executive Head teacher	Chair of Governors

Document control number: CPS075-02

Current Pupil Acceptable Use Agreement/Online Safety Rules

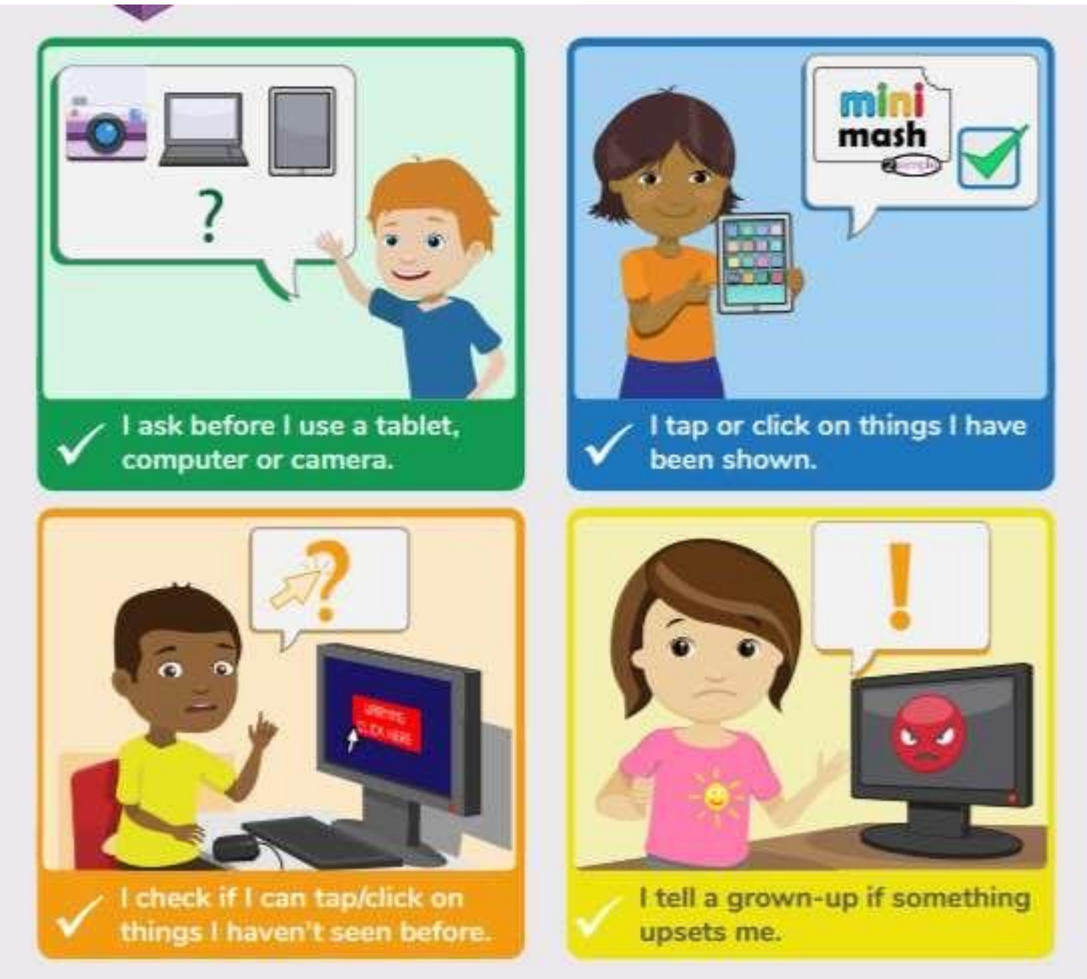
Dear Parent/Carer

Computing including the internet, email, laptops, digital cameras etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any computing.

Please discuss these Online Safety rules with your child. If you have any concerns, please contact the school which holds a computing policy and an Online Safety policy.

- I will only use computing in school for school purposes.
- I will make sure that all computing contacts with other children and adults are responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my monitor and tell my teacher/parent immediately.
- I will not send to children or adults anything that could be considered unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet anyone who I have met via the internet
- I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
- I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my Online Safety.

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.

KS1 –

□ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
□ I only open activities that an adult has told or allowed me to use.
□ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
□ I keep my passwords safe and will never use someone else's.
□ I know personal information such as my address and birthday should never be shared online.
□ I know I must never talk to with strangers online.
□ I am always polite when I post to our blogs, use our email and other ways to talk with people online.

I understand this agreement and know the consequences if I don't follow it

Online Safety Agreement

Childs name: Class No:

We have discussed this and my child agrees to follow the Online Safety rules and to support the safe use of computing at Chuckery Primary School.

Parent/ Carer Signature

KS2 –

- □ I will only access computing equipment when a trusted adult has given me permission and is present □ I will use devices at an appropriate time and not for too long e.g. not late at night (before 9pm) □ I will not deliberately look for, save or send anything that could make others upset.
- □ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- □ I will keep my username and password secure; this includes not sharing it with others.
- □ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names
- □ I will always use my own username and password to access the school network and subscription services such as Purple Mash
- □ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
- □ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
- □ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
- □ Before I share, post or reply to anything online, I will T.H.I.N.K.

T= is it true?
H= is it helpful?
I = is it inspiring?
N = is it necessary?
K= is it kind?

- □ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken

I understand this agreement and know the consequences if I don't follow it.

Online Safety Agreement

Childs name: Class No:

We have discussed this and my child agrees to follow the Online Safety rules and to support the safe use of computing at Chuckery Primary School.

Parent/ Carer Signature

APPENDIX 2

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of their computing skills, Chuckery Primary School provides supervised access to the Internet. We believe that the effective use of the World Wide Web is worthwhile and is an essential skill for children as they grow up in the modern world. All children begin the academic year learning about Online Safety and follow the rules to keep them safe when using the internet. These are displayed in the computing suite to remind the children how to use the internet safely and responsibly.

Please would you read the attached Acceptable Use agreement and sign and return the consent form so that your child may use the Internet at school.

Although there are concerns about pupils having access to undesirable materials, we have taken positive steps to reduce this risk in school. Our school Internet provider, 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 school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please telephone the school to arrange an appointment with the Head teacher.

Yours sincerely

Mr J Pearce
Head teacher

APPENDIX C

Staff Laptop Agreement

The laptop remains the property of Chuckery Primary School

The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated.

Only Chuckery Primary School Staff should use the laptop.

Upon the member of staff leaving the school’s employment, the laptop is returned to the School.

Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the head teacher).

When in school and not being used, the laptop must be kept in an office, locked room or drawer. It must not be left in an unlocked, unattended classroom.

Whenever possible, the laptop must be taken out of school and if so not be left in an unattended car. If there is a need to do so it should be locked in the boot.

The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the head teacher with evidence of adequate insurance.

Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.

Any software loaded must not affect the integrity of the school network.

If any removable media is used then it must be checked to ensure it is free from any viruses. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.

If any fault occurs with the laptop, it should be referred to the computing Technician.

The laptop would be covered by normal household insurance. If not it should be kept in school and locked up overnight.

My laptop is a:

The Asset number on my laptop is:

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name ....

Signature: ....

Date: ....

Appendix D

Staff Acceptable use 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 learners 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.

I will use all computing equipment issued to me in an appropriate way. I will not:

- □ Access offensive website or download offensive material.
- □ Make excessive personal use of the Internet or e-mail.
- □ Copy information from the Internet that is copyright or without the owner’s permission.
- □ Place inappropriate material onto the Internet.
- □ Will not send e-mails that are offensive or otherwise inappropriate.
- □ Will not send emails of a personal nature using school agreed systems e.g. email
- □ Disregarded my responsibilities for security and confidentiality.
- □ Download files that will adversely affect the security of the laptop and school network.
- □ Access the files of others or attempt to alter the computer settings.
- □ Update web pages etc. or use pictures or text that can identify the school, without the permission of the head teacher.
- □ Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Chuckery Primary School.
- □ I will only access the system with my own name and registered password, which I will keep confidential.
- □ I will inform the computing Technician as soon as possible if I know my password is no longer confidential.
- □ I will always log off the system when I have finished working. ·
- □ I understand that the school may, in line with policy, check my computer files and e-mails and will monitor all activity on school devices.
- □ My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the head teacher and register the passwords with the head teacher
- □ If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- □ I will not open e-mail attachments unless they come from a recognised and reputable source.
- □ I will bring any other attachments to the attention of the computing technician.
- □ All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
- □ I will report immediately to the head teacher any unpleasant material or messages sent to me.
- □ I understand that a criminal offence may be committed by deliberately accessing Internet sites that contain certain illegal material.
- □ I understand I may face disciplinary action for any use of a school device that is deemed inappropriate.
- □ I will not use the school network or devices for personal financial gain, gambling, political purposes or advertising as these are forbidden.
- □ Storage of e-mails and attachments should be kept to a minimum to avoid unnecessary drain on memory and capacity.
- □ Activity that threatens the integrity of the school computing systems, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name ....

Signature: ....

Date: ....