Moons Moat First School and Nursery

Online Safety Policy

Background and rationale

Why is internet use important?

The internet is a part of everyday life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security. The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does internet use benefit children and enhance learning?

Benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries
- inclusion in the National Education Network which connects all UK schools
- educational and cultural exchanges between pupils worldwide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across networks of schools, support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data with WCC and DfE
- access to learning wherever and whenever convenient

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is

transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming (including becoming a victim of radicalisation) by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive or addictive use which may impact on social and emotional development and learning.
- Exposure to extremist groups who may attempt to steer audience into rigid and narrow ideology that is intolerant of diversity and could lead to radicalisation.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Our school's e-safeguarding policy has been written from a template provided by Worcestershire School Improvement team which has itself been derived from that provided by the South West Grid for Learning.

Section A - Policy and leadership

A.1.1 Responsibilities

Our E-safety policy has been written by the school, building on the Worcestershire County Council model and government guidance. The E-safety policy and its implementation will be reviewed annually and has been agreed by Senior Leadership team and approved by Governors.

The school's E-safety co-ordinators are: **Mrs Crawford, Mrs Kelly and Mrs Moorhouse** (Child Protection and Safeguarding Co-ordinators) and **Miss Betteridge** (Computing co-ordinator)

A.1.2 Responsibilities: Online Safety Coordinator

Our online safety coordinator – Katie Betteridge is responsible to the governors for the day to day issues relating to e-safety. The e-safety coordinators:

- lead the e-safety committee
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provide training and advice for staff
- liaise with the Local Authority
- liaise with local cluster/partnership groups
- liaise with school ICT technical staff
- receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reviews weekly the output from monitoring software and initiates action where necessary
- meets regularly with e-safety Governor to discuss current issues and review incident logs
- attends relevant meetings and committees of Governing Body
- reports regularly to Senior Leadership Team
- receives appropriate training and support to fulfil their role effectively

A.1.3 Responsibilities: Governors

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing body has taken on the role of e-safety Governor which involves:

- regular meetings with the Online Safety Co-ordinator with an agenda based on:
- monitoring of e-safety incident logs
- reporting to relevant Governors committee / meeting

A.1.4 Responsibilities: Head Teacher

- The Head Teacher is responsible for ensuring the safety (including online safety) of all members of the school community, though the day to day responsibility for online is delegated to the Online Safety Co-ordinator
- The Head Teacher and another member of the senior management team will be familiar with the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with online safety incidents (included in section 2.6 below) and other relevant Local Authority HR / disciplinary procedures)

A.1.5 Responsibilities: Classroom based staff

Teaching and Support Staff are responsible for ensuring that:

- they safeguard the welfare of children and refer child protection concerns using the proper channels: **this duty is on the individual, not the organisation or the school**.
- they have an up to date awareness of online safety matters and of the current school online safety policy and practices -linked to KCSiE
- they have read, understood and signed the school's Acceptable Use Agreement for staff (see Appendix 1)
- they report any suspected misuse or problem to the Online Safety Co-ordinator
- they undertake any digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) in a fully professional manner and only using official school systems
- they embed online safety issues in the curriculum and other school activities, also acknowledging the planned e-safety programme

A.1.6 Responsibilities: Computing technicians

The Computing Technicians (Chestnut Infrastructure) is responsible for ensuring that:

- the school's ICT infrastructure and data are secure and not open to misuse or malicious attack
- the school meets the online safety technical requirements outlined in section B.2.2 of this policy (and any relevant Local Authority Online Safety Policy and guidance)
- users may only access the school's networks through a properly enforced password protection policy as outlined in the school's online security policy
- shortcomings in the infrastructure are reported to the ICT coordinator or Head Teacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This e-safety policy has been developed (from a template provided by Worcestershire School Improvement Service) by a working group made up of:

- School Online Safety Coordinator
- Head teacher / Senior Leaders (safe guarding leads)
- Teachers
- Governors (especially the e-safety governor)
- Pupils

Consultation with the whole school community has taken place through the following:

- Staff meetings
- School Council
- INSET Day
- Governors meeting
- Parents evening
- School website and learning platform / newsletters

Schedule for development / monitoring / review of this policy

This online safety policy was approved by the governing body: 2025	
The implementation of this online safety policy will be monitored by the:	*The senior leadership team under the direction of the online safety coordinator* *OR* *(Miss Crawford, Miss Betteridge, Senior Leadership Team, Governing Body)*
Monitoring will take place at regular intervals:	Termly
The governing body will receive regular reports on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) as part of a standing agenda item with reference to safeguarding:	At each Governors' meeting
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*September 2026*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Worcestershire Safeguarding Children Board e-safety representative* *Local Authority Designated Officer* *Worcestershire Senior Adviser for Safeguarding Children in Education* *West Mercia Police*

A.2.2 Policy Scope

This policy applies to **all members of the school community** (including teaching staff, wider workforce, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, **both in and out of 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 cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

A.2.3 Acceptable Use Agreements

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

- Pupils (EYFS + KS1 / KS2)
- Staff (and volunteers)
- Parents / carers
- Community users of the school's ICT system

Acceptable Use Agreements are introduced at parents' induction meetings and signed by all children as they enter school (with parents possibly signing on behalf of children below Year 2) Children resign on entering KS2.

All employees of the school and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work.

Community users sign when they first request access to the school's ICT system.

Induction policies for all members of the school community include this guidance.

A.2.4 Self Evaluation

Evaluation of online safety is an ongoing process and links to other self evaluation tools used in school in particular to pre Ofsted evaluations along the lines of the Self Evaluation Form (SEF). The views and opinions of all stakeholders (pupils, parent, teachers …) are taken into account as a part of this process.

A.2.5 Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT policies

Computing Policy	How ICT is used, managed, resourced and supported in our school.
Online Safety Policy	How we strive to ensure that all individuals in school stay safe while using Learning Technologies. The e-safety policy constitutes a part of the ICT policy.
School systems and Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect school systems. This links strongly and overlaps with the online safety policy.
Acceptable Use Policy Agreement	An agreement signed by parents, pupils and all staff members and volunteers.
The use of Artificial Intelligence in school	How AI is used to enhance outcomes and educational experiences as well as to support staff in reducing workload.

Other policies relating to Online Safety

Anti-bullying/Anti-cyber bullying	How we strive to eliminate bullying – link to cyber bullying
PSHE	Online Safety has links to staying safe
Safeguarding	Safeguarding children electronically is an important aspect of E-Safety. The online safety policy forms a part of the school's safeguarding policy
Behaviour	Positive strategies for encouraging e-safety and sanctions for disregarding it.
Use of images	**WCC guidance to support the safe and appropriate use of images in schools and settings**
GDPR	

A.2.6 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context **(those in bold are illegal)** and that users should not engage in these activities when using school equipment or systems (**in or out of school**).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images (illegal - The Protection of Children Act 1978)**
- **grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)**
- **possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)**
- **criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)**
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- 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

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the school:

- Using school systems to undertake transactions pertaining to a private business
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Chestnut Infrastructure and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)

- On-line gambling
- Non educational gaming (i.e. Roblox, Fortnite, and other such games)
- On-line shopping / commerce
- Use of social networking sites (other than in the school's learning platform or sites otherwise permitted by the school)

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. Please see Appendix 2.

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 indicated on the following pages:

	Refer to:					**Inform:**	**Action:**		
Pupil sanctions *Schools should edit this table as appropriate to their institution.* *The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.*	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Parents / carers	Remove 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).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔					✔	✔		
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	

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

Staff sanctions

Schools should edit this table as appropriate to their institution.

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

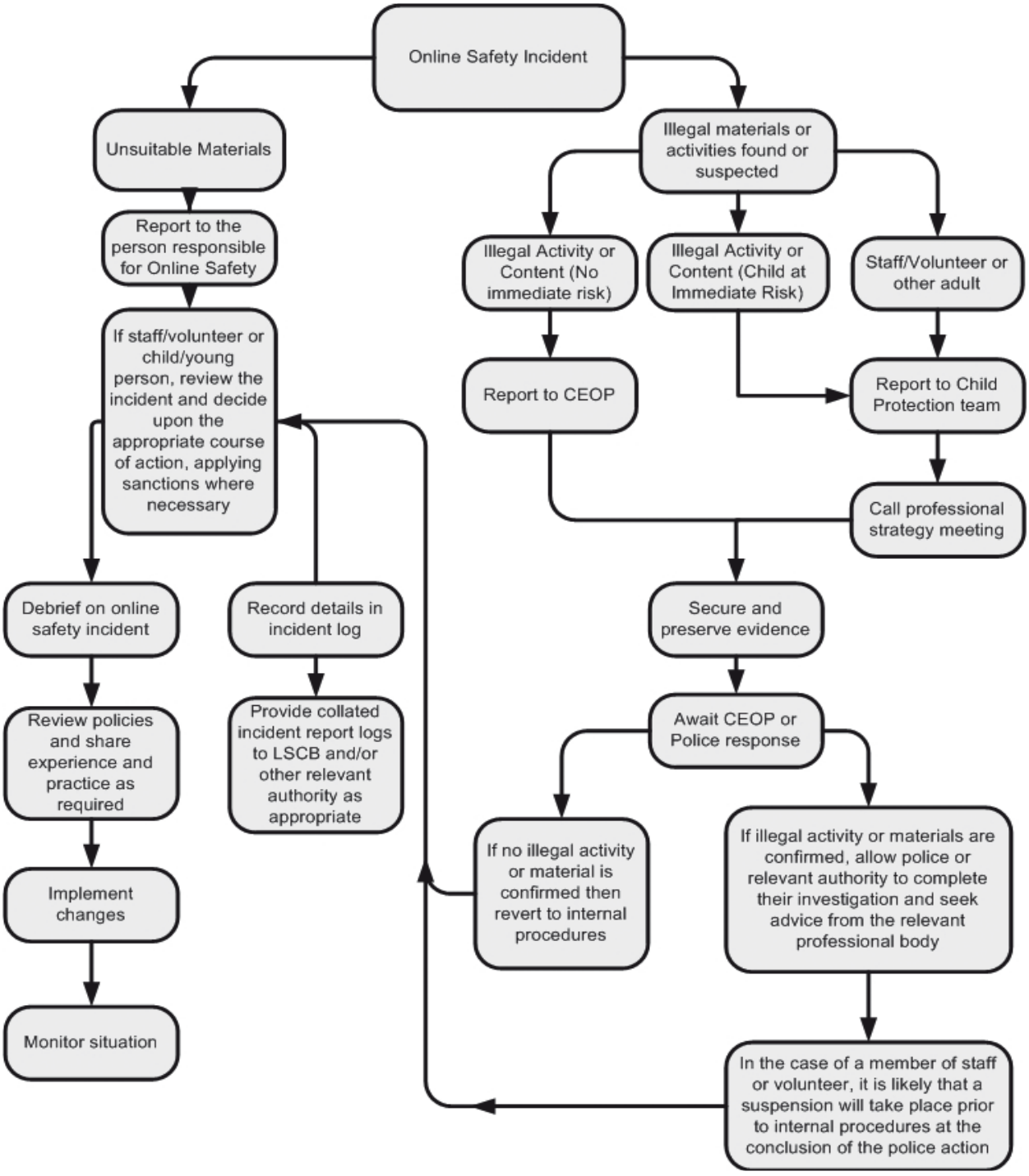
	Refer to:					**Action:**		
	Line manager	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔	✔				✔		
Unauthorised downloading or uploading of files	✔				✔	✔		
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	✔	✔			✔	✔	✔	

Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔	✔		✔	✔	✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔				✔	✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✔	✔			✔			
Actions which could compromise the staff member's professional standing	✔	✔						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔					✔		
Using proxy sites or other means to subvert the school's filtering system	✔				✔	✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations	✔					✔		
Continued infringements of the above, following previous warnings or sanctions	✔	✔			✔			✔

A.2.7 Reporting of online safety breaches

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section A.2.6 of this policy


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
Review policies and share experience and practice as required
Implement changes
Monitor situation
Record details in incident log
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Secure and preserve evidence
Await CEOP or 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 prior to internal procedures at the conclusion of the police action

A.3.1 Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

- ✓ Members of staff are permitted to bring their personal mobile devices into school.
- ✓ Personal hand held devices will be used in lesson time/play time only in an emergency or extreme circumstances with permission from the Head Teacher. Personal phones should not be in classrooms but be stored in lockers in the office area.
- ✓ Members of staff are free to use these devices outside teaching time, when children are not present.

- Pupils are not currently permitted to bring their personal hand held devices into school. If a parent wishes their child to bring a phone to school due to walking to and from school alone (Year 4), this must be requested and an agreement signed. The phone must be stored securely in the office and returned to the child as they leave at the end of the day.

	Staff / adults				Pupils			
Personal hand held technology *It is important that schools review this table in the light of principles agreed within their own establishment.*	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 school	✔							✔
Use of mobile phones in lessons				✔				✔
Use of mobile phones in social time	✔							✔
Taking photos on personal phones or other camera devices				✔				✔
Use of hand held devices e.g. PDAs, gaming consoles				✔				✔

A.3.2 Use of communication technologies

A.3.2a - Email

Access to email is provided for all users in school via Outlook 365 using their personalised institute email.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access)
- Users need to be aware that email communications may be monitored
- Pupils normally use only a class email account to communicate with people outside school and with the permission / guidance of their class teacher
- A structured education program is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email (see section C of this policy)
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (if they are not blocked by filtering)
- Users must immediately report to their class teacher / e-safety coordinator – in accordance with the school policy (see sections A.2.6 and A.2.7 of this policy) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and they must not respond to any such email.

	Staff / adults				Pupils			
Use of Email *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of personal email accounts in school / on school network		✔						✔
Use of school email for personal emails		✔						✔

A.3.2b - Social networking (including chat, instant messaging, blogging etc)

	Staff / adults	Pupils

Use of social networking tools *It is important that schools review this table in the light of principles agreed within their own establishment.*	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Use of non educational chat rooms etc				✔				✔
Use of non educational instant messaging				✔				✔
Use of non educational social networking sites				✔				✔
Use of non educational blogs				✔				✔

A.3.2c - Videoconferencing

Desktop video conferencing and messaging systems linked to Chestnut Infrastructure Broadband via MS Communicator is the preferred communication option in order to secure a quality of service that meets school curriculum standards.

Videoconferencing equipment in classrooms must be switched off when not in use and not set to auto answer.

External IP addresses should not be made available to other sites.

Only web based conferencing products that are authorised by the school (and are not blocked by internet filtering) are permitted for classroom use.

Videoconferencing is normally supervised directly by a teacher. In the event of this not being the case pupils must ask permission from the class teacher before making or answering a videoconference call.

Permission for children to take part in video conferences is sought from parents / carers at the beginning of the pupil's time in school (see section A.2.3 and Appendix 1). Only where permission is granted may children participate.

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services are only issued to members of staff.

A.3.3 Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; **the personal equipment of staff should not be used for such purposes**.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section (A.3.4) for guidance on publication of photographs

A.3.4 Use of web-based publication tools

Our school uses the public facing website www.moonsmoat.worcs.sch.uk only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of children. All users are required to consider good practice when publishing content.

- Personal information will not be posted on the school website and only official email addresses will be used to identify members of staff (never pupils).
- Only pupil's first names will be used on the website, and only then when necessary.
- Detailed calendars will not be published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - ✓ pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
    - ✓ where possible, photographs will not allow individuals to be recognised
    - ✓ written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see section A.2.3 and Appendix 1)
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

A.3.4b – Learning Platforms (Purple Mash)

Class teachers monitor the use of the learning platform by pupils regularly during all supervised sessions, but with particular regard to messaging and communication.

Staff use is monitored by the super-user/administrator.

User accounts and access rights can only be created by the school administrator

Pupils are advised on acceptable conduct and use when using the learning platform.

Only members of the current pupil, parent/carers and staff community will have access to the learning platform.

When staff, pupils, etc leave the school their account or rights to specific school areas will be disabled (or transferred to their new establishment if possible / appropriate).

Any concerns with content may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.

b) The material will be removed by the site administrator if the user does not comply.

c) Access to the learning platform may be suspended for the user.

d) The user will need to discuss the issues with a member of SLT before reinstatement.

e) A pupil's parent/carer may be informed.

A visitor may be invited onto the learning platform by the administrator following a request from a member of staff. In this instance there may be an agreed focus or a limited time slot / access.

Parents sign a contract in order for children to be given access to the learning platform at home, which states that parents/carers must supervise and monitor activity and use of the learning platform at home, therefore ensuring that parents/carers take some responsibility.

A.3.5 Professional standards for staff communication

In all aspects of their work in our school, teachers abide by the broad **Professional Standards for Teachers.**

These will be superseded by the **Teachers' Standards** as described by the DfE:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/301107/Teachers__Standards.pdf

Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and pupils or parents / carers (email, chat, learning platform 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 public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Section B. Infrastructure

B.1 Password security

This is dealt with in detail in our school's ***E-security Policy***. Please refer to that document for more information.

The school's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of school (see section C of this policy).

B.2.1 Filtering

Worcestershire school/academies automatically receive internet filtering via the Worcestershire broadband network if they have opted for the service. This is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. The current Worcestershire filtering service provides flexibility for establishments to decide on their own levels of filtering security. It is possible to add to or override some of the sites filtered centrally. This functionality can be switched on for individual establishments where it is requested providing certain requirements have been met and the school can demonstrate that it is aware of the implications and processes involved. Schools/academies should use this flexibility to meet their learning needs and reduce some of the frustrations occasionally felt by users who wish to maximise the use of the new technologies.

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

As a school buying broadband services from Netbuilder Education/Chestnut Infrastructure, we automatically receive the benefits of a managed filtering service, with some flexibility for changes at local level.

It is recognised that the school can take full responsibility for filtering on site but current requirements do not make this something that we intend to pursue at this moment.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school's filtering policy is held by the **online safety coordinator** (with ultimate responsibility resting with the **Head Teacher and Governors**). They manage the school filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard Worcestershire school filtering service must

- be logged in change-control logs

- be reported to a second responsible person *(the Head Teacher / Computing coordinator [if they are not also the Online Safety coordinator] / Online Safety Governor)* within the time frame stated in section A.1.3 of this policy
- *be reported to, and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change).*

All users have a responsibility to report immediately to class teachers / Online Safety Coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's Online Safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement, Internet permission forms and through online safety awareness sessions / newsletters.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at school, the process to unblock is as follows:

- The teacher makes the request to the school e-safety coordinator.
- The e-safety coordinator checks the website content to ensure that it is appropriate for use in school.

THEN (if the school is not controlling its own filtering)

- If agreement is reached, the e-safety coordinator makes a request to the Chestnut Infrastructure team
- The helpdesk will endeavour to unblock the site within 24 hours. This process can still take a number of hours so teaching staff are required to check websites in advance of teaching sessions.
- Chestnut Infrastructure staff may then be notified of websites that have been unblocked to review them in partnership with the Team. If sites are found to not be appropriate, access will be discussed with the school and then removed.

The Online Safety Coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site's content:

- The site promotes equal and just representations of racial, gender, and religious issues.
- The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.
- The site does not link to other sites which may be harmful / unsuitable for pupils.

• B.2.1e – Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the. Monitoring takes place as follows:

- Identified member(s) of staff (Miss Betteridge and Mrs Crawford) review the Smooth Wall console captures weekly
- "False positives" are identified.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

• B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

- the online safety governor within the timeframe stated in section A.1.3 of this policy
- the online safety committee (see A.1.1)
- the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

B.2.2 Technical security

This is dealt with in detail by Chestnut Infrastructure. Please see that document for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail by Chestnut Infrastructure. Please see their document for more information.

Teachers frequently discuss issues relating to data security and how it relates to staying safe in and out of school (see section C of this policy)

Section C. Education

C.1.1 Online safety education

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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Moon's Moat First School ensures an effective whole school approach to online safety to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

-Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

-Contact: being subjected to harmful online interaction with other users; for example: peer to peer 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: 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.

-Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

These four categories form the framework of our Online Safety Curriculum which is delivered through Computing and PSHE lessons as well as in our vigilance to safeguarding and protecting children.

Online safety education will be provided in the following ways:

- A planned online safety programme is provided as part of computing, PHSE and other lessons. This is regularly revisited, covering the use of ICT and new technologies both in school and outside school
- We use the resources on the National College website as well as CEOP, child line, NSPCC, Natterbox and childnet websites, amongst others.
- Thorough half termly plans are in place for teaching online safety using The National College lesson plans.
- Key online safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use of ICT both within and outside of school.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Staff using YouTube as a learning resource MUST check the suitability of the video- including its adverts and comments prior to use in a lesson. It is not good practice to allow children to search on You Tube as content cannot be filtered within the school's internet filtering system; therefore children may be subjected to inappropriate images, videos and language.
- Where pupils are allowed to freely search the internet, staff should be **vigilant in monitoring the content of the websites the young people visit**, encouraging children to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary. Child friendly search engines, such as 'Kidrex' and 'google kids' are recommended.
- Pupils will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

C.1.2 Digital literacy

- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:
    - ✓ Checking the likely validity of the URL (web address)
    - ✓ Cross checking references (Can they find the same information on other sites?)
    - ✓ Checking the pedigree of the compilers / owners of the website
    - ✓ See lesson 5 of the Cyber Café Think U Know materials below
    - ✓ Referring to other (including non-digital) sources
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- *We use the resources on CEOP's Think U Know site as a basis for our e-safety education* http://www.thinkuknow.co.uk/teachers/resources/

C.1.3 The contribution of the children to e-learning strategy

- It is our general school policy to encourage children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

C.2 Staff training

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

- Mandatory Safeguarding Training (INSET) for all members of staff and Governors. This takes place annually.
- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- It is expected that some staff will identify online safety as a training need within the performance management process.

- 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 policies which are signed as part of their induction
- The Online Safety Co-ordinator will be CEOP trained.
- The Online Safety Coordinator will receive regular updates through attendance at local authority or other training sessions and by reviewing guidance documents released by the DfE, the local authority, the WSCB and others.
- The Online safety Coordinator will provide advice, guidance and training as required to individuals as required on an ongoing basis.
- External support for training, including input to parents, is sought from Worcestershire School Improvement Learning Technologies Team when appropriate

C.3 Governor training

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

- Attendance at training provided by the Local Authority (Governor Services or School Improvement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The online safety governor works closely with the online safety coordinator and reports back to the full governing body (see section A.1.3)

C.4 Parent and carer awareness raising

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, learning platform
- Parents evenings

C.5 Wider school community understanding

- The school offers family learning opportunities in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e-safety should also be targeted towards grandparents and other. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

- Community Users who access school ICT systems / website / learning platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

Safeguarding / Child Protection

- All staff and Governors have received appropriate safeguarding and child protection training (September 2025). All staff have read the following:
- Keeping Children Safe in Education 2025
- What to do if you're worried that a child is being abused
- Staff Code of Conduct
- Safeguarding and Child Protection Policy

Other related policies have been signposted such as Working Together to Safeguard Children, Anti-Bullying, Anti-Cyber Bullying Policy, Behaviour Policy, Critical Incidents, Health & Safety etc.

Staff working with children should maintain an attitude of 'it could happen here' where safeguarding is concerned. If staff have any concerns about a child's welfare, they should act upon them immediately. They should follow the school's policy and procedures and speak with the Designated Safeguarding Lead (Mrs Crawford) or one of the Deputy Safeguarding Leads (Mrs Kelly, Mrs Moorhouse or Mrs Lawrence). In the absence of these staff members, a member of the SLT should be contacted. All concerns should be acted upon and recorded on CPOMS.

Policy approved by Headteacher

Policy approved by the Governing body

The date for the next policy review is September 2026