St Luke's CE First School
Online Safety Policy

This policy is reviewed at least every three years by the governing body and was last reviewed:

on: 20th March 2025

Next Review Date: March 2028

Our School Vision

In our St Luke's family, we recognise we are all God's children and through our caring and nurturing environment, we follow His word. We trust and rely on God's teaching so that we can encourage each other, develop our relationship with one another and the world, and flourish in all that we do.

God's word is a lamp to my feet and a light to my path. (Psalm 119 v.105)

Biblical theology:

We are all God's family and we know that God wants us to succeed in all that we do. It is through his strength that we can do these things and we encourage each other to see that they can be anything they want to be and do anything they want to do.

Please refer to our vision statement and core values (school website; vision and values)

Policy Background and rationale

The potential that technology has to impact on the lives of all of us increases year on year. This is probably even more true for children and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people 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 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.

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

Section A - Policy and leadership

This section begins with an outline of the key people responsible for developing our Online Safety Policy and keeping everyone safe with technology. It also outlines the core responsibilities of all users of ICT in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of technology.

A.1.1 Responsibilities: The Online Safety committee

Our school has an Online Safety committee led by our Online Safety coordinator and made up of pupils from KS1 and KS2 and our Online Safety governor. It meets on a regular basis to:

- Review and monitor this Online Safety policy
- Consider any issues relating to school filtering.
- Discuss any Online Safety issues that have arisen and how they should be dealt with.
- Support and develop Online safety awareness within the school community

Issues that arise are referred to other school bodies as appropriate and, when necessary, to bodies outside of the school.

A.1.2 Responsibilities: Online Safety coordinator

Our Online Safety coordinator is the person responsible to the headteacher and governors for the day to day issues relating to Online Safety.

The Online Safety coordinator:

- leads the Online Safety committee
- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff and users are aware of the procedures that need to be followed in the event of an Online Safety incident
- provides training and advice for staff and other users
- liaises with the Local Authority
- liaises with school ICT technical staff or School Administrator who supports technical issues in school
- meets regularly with the Online Safety governor to discuss current issues and review incident logs
- attends relevant meetings and committees
- 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 (or a governors' subcommittee) receiving regular information about Online Safety incidents and monitoring reports. A member of the governing body has taken on the role of Online Safety governor which involves:

A.1.4 Responsibilities: Headteacher

- The Headteacher is responsible for ensuring the safety (including Online Safety) of all members of the school community, though the day to day responsibility for Online Safety is delegated to the Online Safety Co-ordinator.
- The Headteacher receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- The Headteacher reviews weekly the reports from 'Smoothwall Monitor', our monitoring software and initiates action where necessary
- The Headteacher and Assistant Headteacher 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.

A.1.5 Responsibilities: Classroom based staff

Teaching and Support Staff are responsible for ensuring

that:

- they safeguard the welfare of pupils and refer child protection concerns using the proper channels: **this duty is on the individual, not the school.**
- 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 school Acceptable User Agreement for staff and other users
- 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 systems
- they embed Online Safety issues in the curriculum and other activities, also acknowledging the planned Online Safety programme as part of PSHE

A.1.6 Responsibilities: ICT technician

The ICT Technician is responsible for ensuring that:

- the school 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 schools networks through a properly enforced password protection policy as outlined in the schools Acceptable User policy.
- shortcomings in the infrastructure are reported to the Computing coordinator, Finance Administrator or Headteacher so that appropriate action may be taken.

A.2.1 Policy development, monitoring and review

This Online Safety policy has been developed by a working group made up of:

- Online Safety Coordinator

- Head teacher / SLT

  (DSL's)
- Teachers
- Support Staff
- Governors (especially the Online Safety governor)

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

- Staff meetings
- Online Safety Council
- Training Days
- Governor's meeting / subcommittee meeting
- monitoring of Online Safety incident logs
- reporting to relevant Governors committee / meeting

Schedule for development / monitoring / review of this policy

The implementation of this Online Safety policy will be monitored by the:	The Online Safety co-ordinator and Senior leadership team.
Monitoring of this policy will take place at regular intervals:	Every 3 years
The governing body will receive regular reports on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) as part of a standing agenda item with reference to safeguarding:	Annually
The Online Safety policy will be reviewed every 3 years, or more regularly in the light of any significant new developments in the use of technology, new threats to Online Safety or incidents that have taken place.	Every 3 years
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	Worcestershire Safeguarding Children Board 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 community (including teaching staff, non-teaching staff and admin, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of schools ICT systems, both in and out of the establishment.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off 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 out of the 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 Safeguarding, 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.

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 User Agreement (AUA), 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 and KS1 and KS2
- Staff (and volunteers)
- Community users of the school ICT system

Acceptable Use Agreements are introduced at the beginning of each new school year to each class.

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

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

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. The views and opinions of all stakeholders (pupils, parents / carers, teachers) are considered 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 Computing and Technology Enhanced Learning 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 Online Safety policy constitutes a part of the Computing policy.
School systems and Data Security Policy	How we categorise, store and transfer sensitive and personal data and protect systems. This links strongly and overlaps with the Online Safety policy.

Other policies relating to Online Safety

PSHE	Online Safety has links to staying safe
Safeguarding	Safeguarding pupils electronically is an important aspect of Online Safety. ***The Online Safety policy forms a part of the school's safeguarding policy***

A.2.6 Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in an education context **(those in blue 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, transfer data, 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/academy or brings the school into disrepute

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

- *Using school systems to undertake transactions pertaining to a private business*
- *Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Worcestershire County Council, 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 and non-educational gaming*
- *On-line shopping / commerce unless directly related to school*

  Use of social networking sites whilst in 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 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	Online Safety coordinator	Refer to head teacher	Refer to Police	Refer to Online 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 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

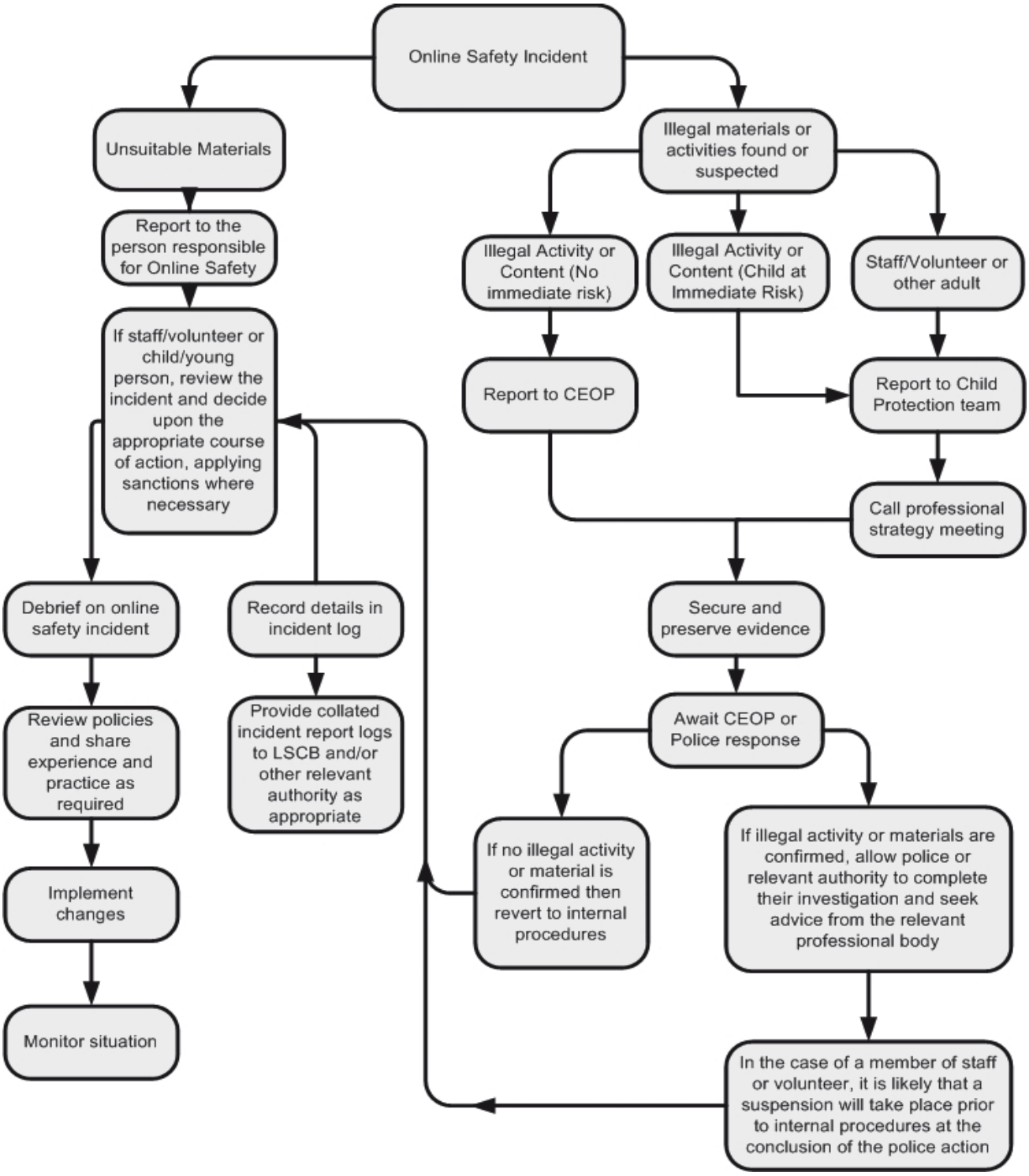
The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	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/academy	✔	✔				✔		
Using proxy sites or other means to subvert the school 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, 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



A.3.1 Use of hand-held technology (personal phones, I-pads and other 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. These should be kept in lockers provided for staff. Staff are to speak to the Headteacher if they need to have their personal mobile devise with them in the classroom, for an emergency reason.

Broadly speaking this is:

- Personal hand-held devices will be used in lesson time only in an emergency or extreme circumstance
- Members of staff are free to use these devices outside teaching time (Break and lunchtimes, when there are no children present)
- A school mobile phone is available for all professional use (for example when engaging in off-site activities). Members of staff should **not** use their personal device for school purposes except in an emergency.
- Devices such as SMART watches should not be active during teaching time. SMART watches should be turned to aeroplane mode during teaching time, but can be switched on during break times.
- Pupils are not permitted to bring their personal hand-held devices into school.
- A number of such devices are available in school (e.g. class I-Pad and cameras) and are used by pupils as considered appropriate by members of staff.
- Children are not permitted to bring their own cameras on trips.

	Staff/adult				Pupils			
Personal hand held technology	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	Not allowed
Mobile phones may be brought into the school	✔							✔
Use of mobile phones in lessons (except in an emergency)		✔	✔					✔
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 school users via Microsoft Outlook.

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

- Staff and pupils should use the school email services to communicate with others regarding school business when in school, or out of school (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 with guidance from their 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)
- Users must immediately report to their teacher / Online Safety coordinator – in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such email.

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

	Staff / adults				Pupils			
Use of social networking tools	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff	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

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 teacher before making or answering a videoconference call.

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

Only key administrators have access to videoconferencing administration areas.

Unique log on and password details for the educational videoconferencing services

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 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.
- Staff should be aware of pupils for whom it has been deemed inappropriate to take and share/publish their photograph (e.g. some children who are looked after)
- 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

A.3.4a - Website (and other public facing communications)

Our school uses the public facing website only for sharing information with the community beyond our school. This includes, from time-to-time, celebrating work and achievements of pupils. 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 clearly recognised
  - written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers. (see section A.2.3 and Appendix 1)

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**.

Teachers translate these standards appropriately for all matters relating to Online 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

The school Online 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

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. No filtering system can, however, provide a 100% guarantee that it will do so. Our school has a filtering system to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the school filtering policy – Smoothwall, is managed on our behalf by Chestnut Infrastructure, (with ultimate responsibility resting with the **Headteacher and governors**). They manage 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 school filtering service must:

- be logged in change-control logs
- be reported to a second responsible person (the head teacher / Online Safety coordinator / Online Safety governor) within the time frame stated in section A.1.3 of this policy

  or

- be reported to, and authorised by, a second responsible person prior to changes being made

All users have a responsibility to report immediately to class teachers / Online Safety coordinator / Head teacher any infringements of the 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 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 may be informed of the school filtering policy through *Online Safety awareness sessions / newsletter etc.*

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 Online Safety coordinator.
- The Online Safety coordinator checks the website content to ensure that it is appropriate for use in school. **Then**

If agreement is reached, the Online Safety coordinator makes a request to Chestnut – Capita: Broadband Team, or other filtering provider

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 network and on school equipment.

Monitoring takes place as follows:

- Identified members of staff (Head teacher / Online Safety co-ordinator / DSL / DDSL) review the monitoring console captures in turn at least once every half term.
- 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
- 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 in IBS School's System and Data Security advice. Please see that document referred to in the introduction for more information.

B.2.3 Personal data security (and transfer)

This is dealt with in detail in Chestnut's System and Data Security advice. Please see that document referred to in the introduction 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 constant help and support to recognise and avoid Online Safety risks and build their resilience. This is particularly important for helping them to stay safe out of school where technical support and filtering may not be available to them.

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 beyond school
- Key Online Safety messages will be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- We use the resources on the Education for a Connected World website as a source of Online Safety education as well as resources and links on the Think u know website and Safer Internet day site.
- Pupils will be helped to understand the need for the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of ICT both within and outside the school.
- In lessons where internet use is pre-planned, it is best practice that younger pupils should be guided to sites checked as suitable for their use. Processes should be in place, and known to pupils, for dealing with any unsuitable material that is found in internet searches.
- 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 pupils to discuss anything of which they are unsure and implementing the expected sanctions and/or support as necessary.
- 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 on-line 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
    - 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 Online Safety education http://www.thinkuknow.co.uk/teachers/resources/. These are mediated by a CEOP trained teacher.

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

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

Pupils play a part in monitoring this policy (see section A.1.1)

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:

- A planned programme of formal Online Safety training will be made available to staff.
- 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 Agreements, which are signed as part of their induction
- The Headteacher and 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, OFSTED, the WSCB and others.
- All teaching staff have been involved in the creation of this Online Safety policy and are therefore aware of its content
- 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 appropriately qualified persons when required.

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, Online 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 Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their 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).

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

- Letters, newsletters, website
- Parents evenings or information sessions
- Reference to the parents materials on the Think U know, National Online Safety or other sites.
- Information via social media to relevant sites such as, National Online Safety.

C.5 Wider community understanding

Messages to the public around Online Safety should also be targeted towards grandparents and other adults engaging with pupils. Everyone has a role to play in empowering young people to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep them safe in the non-digital world.

Community Users who ever access school ICT systems / website as part of Extended school provision will be expected to sign an Acceptable Use Agreement (see Appendix 1) before being provided with access to school systems.

Review

This policy will be subject to the normal cycle of policy review and will be reviewed and ratified by the Governing Body every 3 years. Furthermore, there may be occasions where this policy is reviewed outside the normal review cycle, including but not limited to:

- a change in the Schedule for Inspections
- a change in legal position framework for Online Safety policies.