GLASTONBURY THORN SCHOOL

‘Every day getting better in every way’

ONLINE SAFETY POLICY

Origin	GTS
Committee	Full Governing Body
Date policy approved	15th November 2022
Responsibility for Review	Headteacher
Date policy reviewed	September 2025
Date for next review	September 2026

Revision History			
Version	**Date**	**Author**	**Summary of Changes**
1	June 2022	J Cursley	Contacts updated
			MASH referral added to safeguarding statement
			DSL in attendance when an outside agency is required to interact with a child
			Domestic Abuse – child is treated as a victim and not just a witness
2	September 2022	J Cursley	Updated to 2022 where Computing Lead has signed
3	September 2023	T Redman J Cursley	Updated following KCSIE 2023
4	February 2025	J Cursley	E Safety changed to Online Safety
5	September 2025	T Redman	Online safety changes , KCSIE changes EYFS changes

This policy should be read in conjunction with:

- Child Protection Policy

Rationale - What is Online Safety?

- Online Safety encompasses Internet technologies and electronic communications. This policy highlights the need to educate children about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

- This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: Computing, Child protection, Behaviour, Health and Safety, Anti-bullying, PHSE, Social Networking Policy and Remote learning policy.

- This policy has been developed out of guidance issued by the Department for Education.

- Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' -2025(KCSIE) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy.

- The Governing body will ensure that the filtering and monitoring system is fit for purpose and reviewed annually. They will ensure conversations with the IT provider and E-safety lead take place to check on the suitability of the system.

- The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

- The Designated Safeguarding Lead will take lead responsibility for filtering and monitoring within the school, ensuring that all staff understand their role within this.

TEACHING & LEARNING

Why is Internet use important?

- 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 use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.
- Children use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.
- We endeavour to embed online-safety messages across the curriculum whenever the internet and/or related technologies are used. These messages will be appropriate to the age of the children being taught.
- Children need to understand how to use the internet safely and how to report concerns through school and directly to CEOP.

How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between children world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for children and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including video conferencing and email
- Exchange of curriculum and administration data with MKC and DfE.

How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of children.
- Children will be taught what constitutes acceptable Internet use and given clear objectives for Internet use. Due to the age of our children, they are not permitted to access the internet without an adult being present.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of children.
- Staff should guide children in on-line activities that will support the learning outcomes planned for the children's age and maturity.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will children learn to evaluate Internet content?

- If staff or children discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the Computing subject lead. Children must follow the procedure for reporting unsuitable Internet content (Appendix 1 and 2) which is shared with all children by their class teacher.
- The school will ensure that the copying and subsequent use of Internet-derived materials by staff and children comply with copyright law.
- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Children will be taught the difference between misinformation and disinformation, applying critical thinking skills to discern the difference
- The evaluation of on-line materials is a part of every subject.
- Children will be taught specific skills to keep them safe online through our annual 'Safer Internet day,' and throughout the year where they will participate in a range of activities designed to make them aware of potential hazards when online and how to deal with these.

Who is responsible for the delivery of Online-Safety within school

Key responsibilities of all staff:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up

- Raise awareness of online safety with children in EYFS, supporting parents to understand the risk, initiate safeguards such as parents controls and how to respond to the risks online
- Know who the Designated Safeguarding Lead (DSL) and Computing Lead are
- Governors must ensure that the filters continue to be fit for purpose, allowing staff and children to access relevant research whilst picking up and blocking inappropriate materials.
- DSL takes lead responsibility for internet and filtering and monitoring within the school.
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff code of conduct
- Support staff and children to understand cybercrime and that care must be taken if opening up emails, apps or information from unknown sources.
- Notify the DSL/CL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL/CL what appropriate filtering and monitoring policies are in place)
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use agreement, including the remote learning responsible user agreement for pupils, remind them about it and enforce school sanctions
- Notify the DSL/CL of new trends and issues before they become a problem
- Receive regular updates from the DSL/CL and have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Follow the remote learning policy and teacher protocols during any part or full school closure

MANAGING INFORMATION SERVICES

How will our ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security and annually with IT providers to ensure it continues to be fit for purpose
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the service provider or Local Authority, particularly where a wide area network connection is being planned.
- Use of data storage facilities (such as flash drives) by children within school is prohibited

to protect
against virus transfer.

- AI is increasingly becoming a tool usd in and out of school. Any use of AI must be checked for accuracy and appropriateness
- Files held on the school's network will be regularly checked.
- The Computing Subject Leader/ Network Manager will ensure that the system has the capacity to take increased traffic caused by Internet use.
- Our server is managed by an external service provider.

How will e-mail be managed?

- Children do not have access to a school-based email account. Access in school to external personal e-mail accounts is also blocked.
- Staff should not use their own devices or personal email to contact parents and children.
- All teaching staff have individual school-based email accounts with their own log on. If e-mails are sent to external organisations on behalf of the children or the school, they should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.

How should Website content be managed?

- The point of contact on the Website will be the school address, school e-mail and telephone number. Staff or children's personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school.
- The Website should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Our school website also has a direct link to 'CEOP' (Child Exploitation and Online Protection Centre) on the home page for anyone to report any concerns they may have regarding online behaviour or activity.
- Emails are monitored for content by the school filtering system, this will be reported through to DSL for follow up.

Can children's images or work be published?

- All parents/guardians will be asked to give permission to use their child's photo in publicity materials, on the school website, media and our Facebook page. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/Carers may withdraw permission, in writing, at any time.
- Images which include children will be selected carefully and only those children whose written parental permission has been sought will be identifiable.
- Children's full names will not be used on the website when associated with photographs, or in any way which may be to the detriment of children.
- Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes school outings/visits. School's own mobile devices must be used in this case.
- Images of children will only be kept for a reasonable period of time and deleted when children have left the school.

How will social networking be managed?

- The school has blocked access to social networking sites.
- Staff should notify the DSL if they see comments about the school or pupils being published on social media.
- Staff must not accept friend requests or communications from learners or their family members past and or present.

See also Social Network Policy

How will filtering be managed?

- The school will work in partnership with parents, MKC and the Internet Service Provider to ensure systems to protect children are reviewed and improved. The responsibility for this sits with Governors.
- If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the DSL and Computing Subject Leader.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal, or is in breach of the Prevent Duty Guidance issued under Section 29 of the Counter-Terrorism and Security Act 2015 must be referred to the IWF (Internet Watch Foundation), CEOP (Child Exploitation and Online Protection Centre), and the Thames Valley Police Prevent Lead.
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. The filtering strategy is selected to suit the age and curriculum requirements of children. It is reviewed on a regular basis.

How can emerging Internet uses be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- New technology such as I-watches should not be used in the classroom.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

POLICY DECISIONS

How will Internet access be authorised?

- All staff and children will initially be granted Internet access.
- Parents will be informed that children will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- Children will not be allowed to use computers with access to the Internet unless they are directly supervised by a member of staff.
- An agreement between school, parent and child will be signed, ensuring that all parties understand acceptable behaviour online.

How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor MKC can accept liability for the material accessed, or any consequences resulting from Internet use.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Staff must ensure that they check any materials that they are using. Materials must are age and developmentally appropriate. Staff must watch any resources before recommending them.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the Online-Safety Policy is implemented and compliance with the policy monitored.

How will online-safety complaints be handled?

- Responsibility for handling incidents will be delegated to a member of the Leadership team.
- Any complaint about staff misuse must be referred to the Headteacher.
- Children and parents will be informed of the complaints procedure.
- Parents and children will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling by senior member of staff/class teacher/teaching assistants;
  - informing parents or carers;
  - removal of Internet or computer access for a period, which could prevent access to school work, held on the system.

How is the Internet used across the community?

- The school will liaise with local organisations and MKC to establish a common approach to online-safety.

COMMUNICATIONS POLICY

How will the policy be introduced to children?

- Through weekly computing lessons children will be taught about the safe use of the internet. They will be taught how to use it safely and what to do if they have concerns so elements of this policy will be covered through their lessons.
- Children will also be introduced to an 'Acceptable Use Agreement' through our 'Safer internet week' which will outline how to keep safe online, this signed agreement will then be shared with their parents. (Appendix 3)
- Children are encouraged to report through any concerns they have about online activity.
- Regular discussions and reminders about internet manners and expectations.

How will the policy be discussed with staff?

- All staff will be given the School Online-Safety Policy and its application and importance explained.
- All staff should receive regular training on internet safety and the school procedures.
- All staff must be aware of the role the DSL has in leading on filtering and monitoring.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff should only operate monitoring procedures on instruction from the Leadership Team.
- Staff training in safe and responsible Internet use, and on the school Online-Safety and Safeguarding
- Staff should understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- All staff are responsible for keeping children safe online whilst in school.
- All staff will receive relevant training, supporting them to understand the risks online, how to support children and parents, how to behave appropriately online and how to report concerns.

Policies will be provided as standard practice.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School Online-Safety Policy through newsletters and the school website.
- Parents will be invited to attend a meeting on the importance of online-safety within the home.
  - School will notify parents of any alerts on internet safety.
- Acceptable Use Agreements will be shared with parents when sent home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This will include pocket guide distribution and suggestions for safe Internet use at home.
- Interested parents will be referred to organisations listed in the online-safety pocket guide.

Expectations of internet use

In order to keep children and staff safe online, it is essential that this is revisted regularly and reviewed.

There are 4 key risks to children online that must be considered:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact: being subjected to harmful online interaction with other users; for example: 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,

and
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/).

In addition, there will be specific risks that emerge because of the use of social media. The DSL will ensure that they keep up to date on these issues and regularly update staff on these concerns.

When online sessions are being used for teaching, training and counselling, it is essential that staff, parents and children are aware of the expectations online, which should be part of an agreement that all parties sign up to.
The agreement covers:

- Written conduct agreement for staff/child & parent
- Risk assessment in place
- Clear understanding of policies and procedures and reporting
- Must be arranged in advance and when absolutely necessary
- All sessions to be approved by SLT
- No recording without permission of all parties
- Clear outcomes for session
- DSL must be able to pop in to sessions
- Appropriate dress to be worn (same standards as classroom)
- Only use public area- living room, kitchen, garden (no bedrooms)
- DSL to oversee all internet concerns raised

Staff should consider:

- Teacher acts as a moderator and role model
- Background should not give away location
- Staff and children should be in living / communal areas
- filters at a child's home may be set at a threshold which is different to the school
- child may not have support immediately to hand at home if they feel distressed or anxious about content
- Having contact details for parent available, in case a child becomes distraught during an online session

The nature of this policy dictates that it will need to be reviewed regularly. Changes will be made immediately if technological or other developments so require. This should reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

Signed : Faye Hughes

Role : Computing Subject Leader

Date : February 2025

Appendix 1

Milton Keynes Council Online-Safety Incident Report Form

Online-Safety Incident Report

Incident No:

Date of Incident:	Location of Incident:

Name of person who discovered / identified incident:

Brief description of incident
Brief description of any action taken at time of discovery

Comments / Notes

Date form sent to Online-Safety Co-ordinator	Signature

Appendix 2

Summary of online-safety Incident Log

Incident Number

Date

Time

Nature of incident

Description of incident

Identified by

Pupil(s) involved

Staff involved
Action taken and by whom

Information recorded / secured

Hardware ID secured?

online-safety Co-ordinator informed (by whom)

School Child Protection Officer informed (date+time) (by whom)

Council Child Protection Officer informed (name+date+time) (by whom)

Parents/Carers informed (date+time) (by whom)

Appendix 3

Glastonbury Thorn School

Key Stage 1: Acceptable Use Agreement

My name is _____

This is how I keep **SAFE online**:	✓
1. I only use the devices I'm **ALLOWED** to	
2. I **CHECK** before I use new sites, games or apps	
3. I **ASK** for help if I'm stuck	
4. I **THINK** before I click	
5. I **KNOW** people online aren't always who they say	
6. I don't keep ~~**SECRETS**~~ just because someone asks me to	
7. I don't change **CLOTHES** in front of a camera	
8. I am **RESPONSIBLE** so never share private information	
9. I am **KIND** and polite to everyone	
10. I **TELL** a trusted adult if I'm worried, scared or just not sure	

My trusted adults at school are _____

_____

My trusted adults at home are_____