Star Primary School

Computing & Online Safety Policy

Author: G Williams	Position: AHT	
Status: [Approved/Draft]		
Last Updated: Summer 2023	Next Review: Summer 2025	Version: 1.0

Computing & Online Safety Policy

Introduction and Overview

Our Computing and Online Safety policy has been written by the school. It also takes into account advice from CPD attended by the schools SLT, safeguarding guidelines and Computing Leaders. It has been agreed and approved by the senior leadership team and governing body.

This policy aims to:

- Set out expectations for all Star Primary School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Intervention Policy or Anti-Bullying Policy)

Computing in the School Improvement Plan

Strategy

The school's use of technology promotes innovative learning by digitally confident students, inspired by skilled and creative teaching. We advocate secure and sustainable use of technology, with first-class systems for communication and administration.

Guiding Principles:

- Our policies and procedures are based on best practice -Intention, implementation and impact are communicated to all stakeholders
- A consistent approach to hardware and software usage across the school and a range of commercial applications are made available
- Strategic developments are discussed with all relevant stakeholders and procurement is controlled, managed and sustainable
- Risk assessments are managed, reviewed and updated and systems are protected against threats to security and safety

Areas of Risk

The main areas of risk for our school community can be summarised in the following three categories;

Content

- Exposure to inappropriate content, biassed online media, online pornography, sexting, exposure to violence, racist language, age ratings and substance abuse.

- Child Sexual Exploitation (CSE) which may occur without the child or young person's immediate knowledge (e.g. through others copying videos or images they have created and posted on social media)
- Lifestyle websites such as pro-anorexia, self-harm and suicide sites.
- Sites that promote intolerance towards others based on their ethnic background, race, religion, gender etc.
- Erroneous Content: children and adults need to understand how to check authenticity, bias and accuracy of online content.

Contact

- Grooming, radicalisation and "stranger danger" through online contacts (social media and websites that promote views that are any of the above).
- Technology used to facilitate offline abuse
- Technology used to facilitate online abuse
- Sexual abuse online
- Sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence)
- All forms of bullying including Cyber Bullying.
- Identity theft, profile hacking and sharing passwords.

Conduct

- Privacy issues such as disclosure of personal information and the promoting of any views that affect community cohesion. [Education and Inspections Act 2006]
- Digital footprint and online reputation.
- Health and well-being such as being aware of how long you spend online.
- Sexting (an act of sending and/or receiving personally intimate messages) also referred to as 'youth produced sexual imagery'.
- Sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse
- Initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).
- Radicalisation and consensual and non-consensual sharing of nude and semi-nude images and/or videos
- Up-skirting, which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm;
- Copyright infringement and knowing how to take care and consideration for intellectual property and ownership including content, music and film downloads.

Policy Scope

This policy applies to all members of the Star Primary community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role. The Education and Inspections Act (2006) empowers any Head Teacher of a school to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers staff to impose direct disciplinary sanctions for inappropriate behaviour. This is pertinent to incidents of cyber bullying, safeguarding or any other online safety incidents which may take place outside of the school grounds but are still linked to membership of the school.

The Education Act (2011) increased these powers with regard to searching for information, the use of electronic devices and the deletion of data. The Counter Terrorism and Security Act (2019) placed new statutory duties on schools which means they must work to prevent children being drawn into extremism. The Computer Misuse Act (1990) which covers the use of computer systems without permission or for inappropriate purposes will also be taken into account within this policy.

Under these acts, action can be taken over issues covered by the behaviour and safeguarding policies. The school will deal with such incidents and associated behaviour within its own policies and where appropriate the anti-bullying policy. Where necessary, parents/carers will be informed of incidents that take place outside of the school.

The Head Teacher may decide to report certain matters to the police if a criminal offence is believed to have been committed.

Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The Head Teacher (Lisle Von Buchenroder) will;

- Support safeguarding leads and technical staff as they review protections for **pupils in the home, pupils in school** and **remote-learning** procedures, rules and safeguards
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a UK GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate IT systems and services including school-safe filtering and monitoring as provided by LGfL, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

- Ensure the school website meets statutory requirements (see appendices for website audit document)

The Designated Safeguarding Leads will;

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"
- the designated safeguarding lead (DSL) takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role
- DSL should ensure the child protection policy should include how your school approaches filtering and monitoring on school devices and school networks
- Work with the HT and technical staff to review protections for **pupils in the home** [e.g. DfE Umbrella scheme or LGfL HomeProtect filtering for the home] and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEND in a college and Senior Mental Health Leads) on matters of safety

and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."

- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning and working procedures and technology, including that the same principles of online safety and behaviour apply
- Work with the headteacher, DPO and governors to ensure a UK GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." – see safetraining.lgfl.net and prevent.lgfl.net
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring work and have been functioning/helping. Broadband and Beyond - WebScreen
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident using Safeguard software
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, e.g.self referral, worry box, Star Primary School Online Safety Portal
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this). LGfL Webscreen filtering, view the appropriate filtering statement here. Talk to the school's technical team. *Whilst they will do the technical work, key decisions on what should be allowed are the responsibility of the DSL who should be careful to keep children safe but "be careful that 'over blocking' does not lead to unreasonable restrictions" (KCSIE). Our Safeguarding Shorts: Filtering for DSLs and SLT twilight provides a quick overview.*

- Facilitate training and advice for all staff, including supply teachers and auxiliary staff:
- all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages
- Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- it would also be advisable for all staff to be aware of Annex D (online safety)
- cascade knowledge of risks and opportunities throughout the organisation
- cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents - share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles

Governors will;

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, they should identify and assign:

- a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, external service providers
- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Governing boards should make sure the designated safeguarding lead (DSL) takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role
- Boards should also make sure all staff understand their expectations, roles and responsibilities around filtering and monitoring as part of safeguarding training
- Governing boards should review the DfE's filtering and monitoring standards. Your board should discuss with your IT staff and service provider what needs to be done to support your school in meeting the standards
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety lead/ DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a UK GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your school
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated […] in line with advice from the local three safeguarding partners […] integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". LGfL's appropriate filtering submission is here
- "Ensure that children are taught about safeguarding, including online safety […] as part of providing a broad and balanced curriculum […] Consider a whole school or college approach to online safety [with] a clear policy on the use of mobile technology." NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS framework 'Education for a Connected World – 2020 edition' to support a whole-school approach.

Computing Leader, Personal Development Team and technical team will;

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the PD lead (s) to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

All Staff will:

- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- 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
- Know who the Designated Safeguarding Lead (DSL) is
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- Read and follow this policy in conjunction with the school's main 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 Acceptable Use Policies
- Notify the DSL 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 as part of a whole school approach in line with the RSHE curriculum, 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 in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and UK GDPR.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online sources and resources before using
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding 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. More guidance on this point can be found in this Online Reputation guidance for schools.
- Read and agree to the privacy notice when using Inventry sign in

RSHE Leads will:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."

- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within RSHE.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Subject leaders will:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework 'Education for a Connected World – 2020 edition and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Ensure subject specific action plans also have an online-safety element

Network Manager / Technician will:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home, pupils at school,** [e.g. DfE Umbrella scheme or LGfL HomeProtect filtering for the home] and **remote-learning** procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Meet the RSHE lead to see how the online-safety curriculum delivered through this subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- Complete Online Safety Audit
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls
- Test systems and user settings regularly
- Network managers/technicians at LGfL schools to ensure the following solutions are in place: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Data Protection Officer will:

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

LGfL Nominated Contacts will:

- To ensure all LGfL services are managed on behalf of the school in line with school policies, following data handling procedures as relevant

- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering and monitoring settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Google Workspace.
- Ensure the DPO is aware of the UK GDPR information on the relationship between the school and LGfL at gdpr.lgfl.net

Volunteers and contractors will:

- Read, understand, sign and adhere to an Acceptable Use Policies (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- Read and agree to the privacy notice and when using Inventry sign in

All Pupils will:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Treat **home learning** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.

- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/Carers and the community will:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their child to follow it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning

- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

- Read and agree to the privacy notice when using Inventry sign in

External Groups will:

- **Key responsibilities:**

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Read and agree to the privacy notice when using Inventry sign in
- Support the school in promoting online safety and data protection

- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers

Handling Complaints

The school will take all reasonable precautions to ensure online safety and empower the children to deal with exposure appropriately. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or handheld device. Neither the school nor the local authority can accept liability for material accessed or any consequences of internet access.

Staff and pupils are given information about infringements and the possible sanctions in place. Sanctions available include;

- Interview (counselling by the School Councillor/Phase Group Leader/ Designated Safeguarding Lead /Deputy Head Teacher/Head Teacher)
- Informing parents/carers.
- Removal of internet and/or computer access for a period of time.
- Referral to the local authority and/or police.

Our Designated Safeguarding Lead acts as a first point of contact for any complaint regarding pupil concerns. Any complaint about staff misuse is referred to the Head Teacher. Complaints about cyber bullying are dealt with in accordance with our anti-bullying policy. Complaints related to child protection are dealt with in accordance with the school and local authority child protection procedures.

The school takes the view that online safety concerns are no different to any other safeguarding concern.

Data Protection and Data Security

“UK **GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**.”

All pupils, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements.

Rigorous controls on the LGfL network, USO sign-on for technical services, firewalls and filtering all support data protection. The following data security products are also used to protect the integrity of data, which in turn supports data protection: USO sign on for LGfL services, Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.

The headteacher, data protection officer and governors work together to ensure a UK GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of USO-FX / Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DPO and DSL should be informed in advance.

We safeguard using / advocating:

- CCTV
- Use of personal vs school devices
- Password policy / two-factor authentication
- Reminders to lock devices when leaving unattended

- Device encryption
- Access to and access audit logs for school systems
- Backups
- Security processes and policies
- Disaster recovery
- Access by third parties, e.g. IT support agencies
- Wireless access
- File sharing
- Cloud platform use, access and sharing protocols

Review and Monitoring

The computing and online safety policy is referenced from within other school policies, safeguarding statements, anti-bullying policies and other educational policies. The school has a Designated Safeguarding Lead, a Computing Leader and technical team who will be responsible for document ownership, review and updates. The Computing and Online Safety policy will be reviewed annually or when any significant changes occur with regards to technology or online threats. The Computing and Online Safety policy has been written by the Computing Leader and checked by the Head Teacher and the Governing Body to ensure that it is current and appropriate for its intended audience and purpose. Any changes to the policy will go through a rigorous process of clarification from the Head Teacher and Governing Body before being edited publicly. Online Safety checks are undertaken each half term and reported to Headteacher / Safeguarding / IT teams and Governing Body. An annual review is undertaken and appropriate remedial measures are put in place.

Online Safety in the Curriculum

Star Primary School has a clear and progressive online safety education programme as part of the Computing and RSHE curriculum. It is built on local authority and LGfL safeguarding, Computing National Curriculum Programmes of Study (2013), Relationships and sex education (RSE) and health education (2021)

. This covers a range of skills and behaviours appropriate to their age and experience including;

- To understand acceptable behaviour when using an online environment (i.e. be polite, no bad or abusive language or other inappropriate behaviour and keeping personal information private)
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings.
- To **STOP** and **THINK** before they **CLICK**
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a website may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- To understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why "on-line friends" may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files without permission.
- To have strategies for dealing with receipt of inappropriate materials.
- To understand why and how some people will "groom" young people for sexual reasons, exploitation and extremism.
- To understand the impact of cyber bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including cyber bullying and extremism and how to seek help if they experience problems when using the internet and related technologies (i.e. parent/carer, teacher/trusted staff member or an organisation such as CEOP, Child Line or the police).
- Planning internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Reminding pupils about their responsibilities through an acceptable usage policy which every student will sign and will be displayed throughout the school and will regularly be displayed when a student logs on to a school computer.
- Running projects and events involving pupils to highlight online safety to parents/carers and pupils.
- Ensuring staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensuring that when copying materials from the web, staff and pupils understand issues around bias, copyright and to know they must respect and acknowledge copyright/intellectual property rights.
- Ensuring that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups, buying online, online gaming and online gambling.
- Providing information and advice signposted on the school website.

Staff and Governor Training

Star Primary School will;

- Ensure staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection - USO-FX credentials
- Make regular training available to staff on online safety issues and the school's online safety education program
- Provide, as part of the induction process, all new staff [including those on university/college placement and work experience] with information on online safety and guidance on the online-safeguarding policy and the school's Acceptable Use policies.

Parent Awareness Training

Star Primary School runs a programme of advice and guidance for parents. This is led by Community Wellbeing Advocate;

- An introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safety behaviour are made clear
- Information leaflets; articles in the school newsletters and on the school website.
- Suggestions for safe Internet use at home.
- Providing information about national support sites for parents.
- Information and advice sign posted on the school website.

Safeguarding and Prevent Strategy

Star Primary School;

- Ensures that through our school vision, values, rules, diverse curriculum and teaching we promote tolerance and respect for all cultures, faiths and lifestyles.
- Ensures that staff understand the issues of radicalisation, are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns.
- Ensures that staff and pupils understand the issues around aspects of grooming, exploitation and radicalisation on the Internet, as age appropriate.
- Is aware that extremists use the internet, including social media, to share their messages and takes appropriate steps to reduce exposure.
- Refer to and keep up to date with our prevent duties as set out below.

Statutory Duties

- The duty to prevent children and young people being radicalised is set out in the following documents.
- Counter Terrorism and Security Act (2019 updated)
- Keeping Children Safe in Education (2023)
- Prevent Duty Guidance (2021 updated)
- Working Together to Safeguard Children (2022 updated)

Non-Statutory Guidance

- Promoting fundamental British values as part of SMSC in schools: Departmental advice for maintained schools (DfE 2014)

Conduct and Incident Management

In this school, all users;

- Are responsible for using the school's computing systems in accordance with the relevant Acceptable Usage Policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- Need to understand the importance of misuse or access to inappropriate materials and be aware of the consequences.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.
- Will be expected to know and understand school policies on the use of mobile phones, smart watches, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

In this school, staff and pupils;

- Are responsible for reading the school's online safety policy and using the school computing systems accordingly, including the use of mobile phones and handheld devices.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

In this school, parents/carers;

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

At Star Primary School;

- There is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions.
- Sanctions are applied according to the policy that applies to that contravention unless a serious incident that involves a criminal act occurs at which point the matter will be directed to the police without regard for internal management procedures.
- All members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- Support is actively sought from other agencies as needed (e.g. LGfL, UK Safer Internet Centre helpline, CEOP) in dealing with online safety issues.
- Monitoring and reporting of e safety incidents takes place and contributes to developments in policy and practice in online safety within the school. The local authority / parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.
- Any incident that indicates that evidence of indecent images or offences concerning child protection involving members of the school community should be immediately referred to the Police. This is to prevent the loss of valuable evidence both on and off the premises by not inadvertently making the suspect aware of raised suspicions.

Managing the Computing Infrastructure

Internet Access, Security & Filtering

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." For example, access to Youtube is restricted to staff only via authentication using their USO credentials. Any content that is hosted on Youtube can then be shared with pupils at an age-appropriate level. Our webscreen filtering is strict for this reason.

At Star, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen, which is made specifically to protect children in schools.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active/Pro-active technology monitoring services

At Star, we have decided that all three are appropriate dependent on the age and needs of the pupils.

At home, school devices are secured with the LGfL HomeProtect home filtering so they can be filtered and monitored when on home wifi connections.

When pupils log into any school system on a personal device, activity may also be monitored here. For example, using Google for Education Workspace with a filtering extension, this will apply when logging into a home Chromebook but also when logging into a Chrome profile on a Windows laptop.

Star Primary School;

- □ Has the educational filtered secure connectivity through the LGfL and so connects to the 'private' National Education Network.
- □ Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- □ Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the pupils.
- □ Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so unauthorised staff and pupils cannot download executable files.
- □ Uses DfE, local authority or LGfL approved systems such as S2S, USO FX, and secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site.
- □ Blocks all chat rooms and social networking sites except those that are part of an educational network or approved learning platform.
- □ Only unblocks other external social networking sites for specific purposes such as Computing or curriculum lessons.
- □ Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level
- □ Uses security time-outs on Internet access where practicable / useful.
- □ Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- □ Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas
- □ Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- □ Ensures pupils only publish within an appropriately secure environment: LGfL secure platforms
- □ Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's learning platform as a key way to direct students to age / subject appropriate web sites
- □ Plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. Google Safe Search.
- □ Never allows/is vigilant when conducting 'raw' image search with pupils e.g. Google image search.
- □ Informs all users that internet use is monitored
- □ Informs staff and pupils that that they must report any failure of the filtering systems directly to the Computing Lead / technical team or escalates as appropriate to the Technical Service Provider or LGfL Helpdesk as necessary.

- Makes clear through staff meetings and teaching programmes that all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – police – and the LA.

Network Management

Star Primary School;

- Uses individual log-ins for all users - the London USO system.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Ensures the Computing Leader and technical team are up-to-date with LGfL services and policies. We also require Newham Partnership Working (Technical Support Provider) to be up-to-date with LGfL services and policies.
- Storage of all data within the school will conform to the UK GDPR requirements.

New and Emerging Technology

Star Primary School;

- Will access new and emerging technologies for educational benefit and a risk assessment taking into account our safeguarding criteria will be carried out before use in school is allowed.

Ensuring the network is used safely

Star Primary School;

- Ensures staff read and sign that they have understood the school's Online Safety policy. Following this, they are set-up with Internet, email access and network access. Staff members have been provided with interactive online safety training. Online access to service is through a unique, audited username and password. We also provide a different username and password for access to our school's network.
- Control Staff access to the schools' management information system through a separate password for data security purposes.
- Give all pupils their own unique username and password which gives them access to the Internet and the learning platform.
- We use LGFL's Unified Sign-On (USO) system for username and passwords.
- Have set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Require all users to always log off when they have finished working or are leaving the device unattended.
- Have blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Make clear that members of staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Make it clear that staff ensure that any device loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Makes clear that staff accessing local authority systems do so in accordance with any corporate policies
- Maintains equipment to ensure Health and Safety is followed
- Have separate curriculum and administration networks, with access to the Management Information System set-up so as to ensure staff users can only access modules related to their role
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / local authority approved systems
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Provides pupils and staff with access to content and resources through the approved learning platform which staff and pupils access using their username and password (their USO username and password).
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- Uses the DfE secure s2s website for all CTF files sent to other schools.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our local authority or through USO secure file exchange
- Follow LGfL advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard enterprise security level /appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.

Personal Password/GMail Accounts

Password Policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems.
- Staff are responsible for keeping their password private.
- We require staff to change their passwords into the MIS and LGfL USO admin site.

GMail

Star Primary School;

- Provides staff with a Gmail account for their professional use, and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@star.newham.sch.uk (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date.
- Will report messages relating to or in support of illegal activities to the relevant authority and if necessary to the police.
- Knows that spam, phishing and virus attachments can make emails dangerous. We use LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils

- Pupils are introduced to email as part of the Computing curriculum.
- Pupils email accounts are restricted and inactive unless express consent is given by the Digital Strategy Manager and Headteacher
- Pupils are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
  - that an e-mail is a form of publishing where the message should be clear, short and concise.
  - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
  - they must not reveal private details of themselves or others in email, such as address, telephone number, etc.
  - to '**Stop** and **Think** before they **Click'** and not open attachments unless they are sure the source is safe.
  - that they should think carefully before sending any attachments.
  - embedding adverts is not allowed.
  - that they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature.
  - not to respond to malicious or threatening messages.
  - not to delete malicious of threatening emails, but to keep them as evidence of bullying.
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them.
  - that forwarding 'chain' e-mail letters is not permitted.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including email and we explain how any inappropriate use will be dealt with.

Staff

- Staff can only use the local authority or LGfL email systems / Gmail on the school system.
- Access in school to external personal email accounts may be blocked.
- Staff use a 'closed' local authority email system which is used for local authority communications and some 'local authority approved' transfers of information.
- Never use email to transfer staff or pupil personal data.
- Staff know that email sent to an external organisation must be written carefully and may require authorisation.
  - the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.
  - All staff are required to sign our local authority / school Agreement Form (AUP) to say they have read and understood the online safety rules, including email and we explain how any inappropriate use will be dealt with.. Staff 'Accept' usage terms and conditions when they first login to their user area. They accept the usage terms and conditions every 12 months.

School Website

- The Head teacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our authorised website managers once approved by the Head teacher.
- The school website complies with the statutory DfE guidelines for publications.
- Most material is the schools' own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@star.newham.sch.uk.
- Home information or individual email identities will not be published.
- Photographs published online do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- Online Safety advice and help is sign posted from the school website to support the whole school community.

Google Drive

- Uploading of information on the schools' Google Drive is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their teacher drive
- Users can only log on to the Google Drive and access the Google for Education Workspace with their staff USO and Google account credentials
- Data stored on our Google Drive will not be shared with external users unless prior consent is given by the Digital Strategy manager
- Access to shared drives is restricted
- Data uploaded to the schools Google Drive will only be accessible by members of the school domain.
- In school, pupils are only able to upload and publish within school approved and closed systems: pupil shared drives and their own personal drive space
- All pupils and staff receive regular CPD around the safe and appropriate use of the Google Workspace
- Data is archived and / or removed annually
- Copies of files and folders are not made unnecessarily
- Our Google Drive complies with our Privacy Notice, Retention Policy and UK GDPR regulations

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained for 30 days), without permission except where disclosed to the police as part of a criminal investigation.
- We only allow footage to be reviewed with written consent from the Head Teacher unless in an emergency requested by the Police. This applies to all staff.
- All images are stored and processed in compliance with the Data Protection Act (2018) and are only kept for a limited period.

Please refer to CCTV Policy

Social Media and Networking

- Teachers are instructed not to run social network spaces for pupil use on a personal basis or to open up their own spaces to their pupils
- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use social media tools with pupils as part of the curriculum will need permission from the Head teacher or SLT before using them in the classroom. They will need to risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- Personal publishing will be taught via age appropriate sites such as Google Sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils will be encouraged to approve and invite known friends on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites.

School staff will ensure that in private use;

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

Official use of Social Media

- Star Primary's official social media channel is Twitter and Instagram.
- Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- Official use of social media sites as communication tools will be formally approved by the Headteacher.
- Approved staff members will use school/setting provided email addresses to register for and manage any official approved social media channels.
- Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislation.
- Acceptable usage training will be provided to approved staff members to ensure that they are aware how to use the social media platforms and ensure that they are used safely and responsibly.
- Social media platforms will only be used to celebrate and showcase activities and workshops, they will not be used as a communication tool.
- Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.
- Official social media use will be in line with existing policies including anti-bullying, child protection and UK GDPR.
- Images or videos of pupils will only be shared on official social media sites/channels in accordance with the media consent policy.
- Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- Official social media sites will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school/setting website and take place with written approval from the Leadership Team.
- Leadership staff must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.

➢ Parents/Carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

➢ Official social media channels will link back to the school/setting website and/or Acceptable Use Policy to demonstrate that the account is official.

➢ The school/setting will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Video Conferencing

Star Primary School;

- Use Google Meet as part of the Google for Education Workspace for video conferencing
- Staff know how to safely deploy ‘host controls’ on any Google Meet
- Staff, parents and pupils follow the rules and guidance for the safe use of Google Meet
- Quick Access is turned off for online parent consultations and external users so only approved hosts can admit entry
- Google Meet links are reset and made invisible to all parents, staff and pupils after each Google Meet via Google Classroom
- Any data breach or inappropriate conduct is reported to the school DPOs: Lisle Von Buchenroder, Gemma Williams and Matthew Norton

Data Security

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Strategic and Operational Practices

At Star Primary School;

- The school is the Data Controller and the Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are assessed using the Disclosure and Barring Service (DBS) and Disqualification by Association (DbA) checks and records are held in one central record e.g. SIMS. We ensure all the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
    - Staff
    - Governors
    - Pupils
    - Parents

This makes clear staff responsibilities with regard to data security, passwords and access.

- We follow local authority guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the local authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any protected and restricted material must be encrypted if the material is to be removed from the school and limit such data removal.
- School staff with access to setting-up usernames and passwords for email, network access and learning platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.
- Regular UK GDPR health checks are undertaken and logged
- Staff receive UK GDPR training every 2 years

Technical Solutions

All staff have access to secure area(s) on the network to store sensitive documents or photographs.

- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes of idle time on the network.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- Staff with access to the Admissions System also uses an LGfL OTP tag as an extra precaution.
- We use RAv3 with its 2-factor authentication for remote access into our systems.
- We use LGfL USO FX to transfer other data to schools in London, such as references, reports of children.
- We use the LGfL secure data transfer system, USO AutoUpdate, for creation of online user accounts for access to broadband services and the London content.
- No back-ups leave the site on mobile devices.
- We use RM remote secure back-up solution for disaster recovery on our network servers.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Portable equipment loaned by the school for use by staff at home, where used for any protected data, is disposed of through the same procedure.
- Paper based sensitive information is shredded, using a cross cut shredder.

Equipment and Digital Content

All school mobile devices that connect through the school’s wireless access points are subjected to the same filtration and monitoring system as those devices that gain access to the internet through conventional authenticate network connections.

Personal mobile phones and mobile devices including wearable technology and BYOD

- Student mobile phones which are brought into school must be turned off (not placed on silent) and handed to the Reception staff on arrival at school. These can be collected at the end of the day.
- Staff members may use their phones during school break times.
- Designated ‘mobile use’ areas are the school staff room and private office spaces
- Mobile phones brought into school are entirely at the staff member, pupil’ & parents’ or visitors' own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile device is to be avoided; except where it has been explicitly agreed otherwise by the Head Teacher. Such authorised use is to be monitored and recorded. All mobile device use is to be open to scrutiny and the Head Teacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- Where parents or pupils need to contact each other during the school day, they should do so only through the school’s telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- The bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent from the Head Teacher.

Pupils’ use of personal devices

- The school strongly advises that pupil mobile phones and other mobile devices should not be brought into school.
- The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety and this applies to Years Five and Six pupils only. Pupils required to bring a mobile phone into school in lower year groups must have consent fro the Headteacher. A written letter of application from the parent is required.
- If a pupil breaches the school policy then the phone or device will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Pupils found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the pupil’s withdrawal from either that examination or all examinations.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child directly during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Personal devices that can store, share and/or transmit data or content should not be brought into school without prior consent from staff. It may be confiscated, searched and any inappropriate content deleted or shared with the authorities by the head teacher or appointed representative.

Staff use of personal devices

- Staff devices must be noted in school – name, make & model, serial number as part of the Asset Register.
- Staff are discouraged from using their own mobile phones or devices for contacting pupils or their families in their professional capacity.
- Staff members are encouraged to use a school phone where contact with pupils, parents or carer is required. If it can’t be avoided staff should use the 141 prefix to avoid disclosing their private number.
- Mobile phones and personally-owned devices should be switched off or switched to ‘silent’ mode.
- Bluetooth communication should be ‘hidden’ or switched off.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by SLT.
- Staff should avoid using personally-owned devices, such as mobile phones or cameras, to take photos or videos of pupils and should only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital Images and Video

At Star Primary School;

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials
- Staff sign the school's Acceptable Usage Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger pupils as part of their Computing scheme of work.
- Pupils and staff are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school.
- We teach them about the need to keep their data secure and what to do if they are subject to bullying, grooming or abuse.

Asset Disposal

- Details of all school-owned hardware are recorded through Meraki – a cloud-based platform
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed.
- The school will only use authorised companies who will supply a written guarantee that this will happen.

Disposal of any equipment will conform to the Waste Electrical and Electronic Equipment Regulations 2018 and/or the Waste Electrical and Electronic Equipment (Amendment) Regulations 2018. Further information can be found on the Environment Agency website.

Additional Information

London Grid for Learning (LGfL) offer advice and guidance on best practice for member schools and we liaise with them closely on a day to day basis.
www.lgfl.net/safety

Child net International, a non-profit organisation, offers advice for children, parents and professionals.
http://www.childnet.com/

Alternatively refer to your Union for advice, support and guidance.