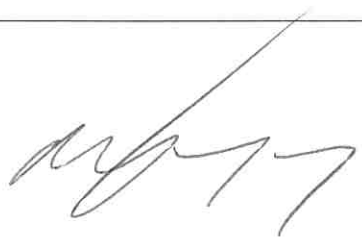
E-SAFETY POLICY

Lakenheath Community Primary School

Version Number	7
Date of Policy	March 2025
Review Date	March 2026
Head Teacher's Signature	
Chair of Governors' Signature	

Document Change History

Version	Date	Change Details
1	July 2016	N/A
2	November 2018	Content review and format change.
3	January 2021	Content review, additional links to GDPR added.
4	March 2022	Policy review, no changes required.
5	March 2023	Complete policy upgrade and review due to advances in eg GDPR and guidance
6	March 2024	Content review, no changes required
7	March 2025	Content review, no changes required

Lakenheath Community Primary School

This policy applies to all members of Lakenheath Community Primary School community (including staff, governors, supply teachers, volunteers, contractors, pupils, parents/carers and visitors) 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.

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2019 (KCSIE), 'Teaching Online Safety in Schools' 2020 and taken advice from other statutory documents: the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. It complements existing and forthcoming subjects including

Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

This policy is a living document and subject to full annual review but will also be amended where necessary during the year in response to developments in our school and the local area. Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct. Many of the new risks are mentioned in KCSIE 2020, e.g. fake news and upskirting we keep updated with prominent new and emerging trends, through following safeblog.lgfl.net. There has been an alarming increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Contact and conduct of course also remain important challenges to address.

In past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some of our pupils may have missed opportunities to disclose such abuse during the first lockdown.

1. Aims

This policy aims to:

- *Set out expectations for all Lakenheath Community 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 and respectful use of technology to support teaching & learning, increase attainment and prepare children 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 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 (in-line with the school's Behaviour & Anti-Bullying Policy)*

2. Roles and 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.

Headteacher Key responsibilities:

- *Support safeguarding leads and technical staff as they review protections for pupils in the home and remotelearning procedures, rules and safeguards*
- *Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding*
- *Oversee the activities of the DSL and ensure that their responsibilities listed 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 DSL 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 staff, DSL and governors to ensure a GDPRcompliant framework for storing data, but helping to ensure that child protection is always put first and dataprotection processes support careful and legal sharing of information*
- *Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles*
- *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 suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised*
- *Ensure the school website meets statutory DfE requirements.*

Designated Safeguarding Lead Key responsibilities:

- *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety) … this lead responsibility should not be delegated." KCSIE 2020*
- *Work with the Headteacher and technical staff to review protections for pupils in the home and remotelearning procedures, rules and safeguards*
- *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." KCSIE 2020*
- *"Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies." KCSIE 2020*
- *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 procedures and technology, including that the same principles of online safety and behaviour apply*
- *Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident*
- *Work with the headteacher, SLT and governors to ensure a 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 safety through receiving regular updates in online safety issues and legislation and be aware of local and school trends and undertake Prevent awareness training*
- *Review and update this policy, other online safety documents 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.*
- *Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles*
- *Ensure that online safety education is embedded across the curriculum and beyond, in wider school life*
- *Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents*
- *Liaise with school technical, pastoral, and support staff as appropriate*
- *Communicate regularly with SLT and the designated safeguarding governor to discuss current issues (anonymised), review incident logs and appropriate filtering and monitoring*
- *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*
- *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*
- *Maintain up-to-date documentation of the school's online security and technical procedures*
- *Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown*
- *Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware*
- *Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, well as to bullying*

Governing Body, led by Safeguarding Governor Key responsibilities:

- *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*
- *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*
- *"Ensure an appropriate senior member of staff, from the school 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..." KCSIE 2020*
- *Support the school in encouraging parents and the wider community to become engaged in online safety activities*
- *Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings*
- *Work with the DSL and headteacher to ensure a 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 and Annex A of KCSIE; check Annex C 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." KCSIE 2020*
- *"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". KCSIE 2020*
- *"Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology."*

In-line with 'Teaching Online Safety in Schools 2019' and the UKCIS cross-curricular framework 'Education for a Connected World' to support a whole-school approach.

All staff Key responsibilities:

- *Since 2020 pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies.*
- *Recognise that a new RSHE scheme has been introduced year 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*
- *Know who the Designated Safeguarding Lead (DSL) is and the Deputy DSLs are*
- *Read Part 1 and Annex A and have been sign posted to Annex C of KCSIE 2020*
- *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.*
- *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 (devices, the internet, 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*
- *When supporting pupils remotely, be mindful of additional safeguarding considerations*
- *To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, 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*
- *Prepare and check all online source and resources before using within the classroom*
- *Encourage pupils to follow their acceptable use policy, at home as well as at school and remind them about it and enforce school procedures if not followed*
- *Notify the DSL of new trends and issues before they become a problem*
- *Take a zero-tolerance approach to bullying and low-level sexual harassment*
- *Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and violence) in the playground, corridors, toilets and other communal areas outside the classroom – always report to the DSL and via CPOMS*
- *Receive regular updates from the DSL 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.*

PSHE Lead Key responsibilities:

- *Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education 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." KCSIE 2020*
- *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 PSHE.*

Computing Lead Key responsibilities:

- *Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum*
- *Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing*
- *Support the HT and DSL team as they review protections for pupils with any remote-learning procedures, rules and safeguards*
- *Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements*
- *Work closely with the DSL to ensure that school systems and networks reflect school policy*
- *Ensure all 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 SLT with support from ICT Support Team*
- *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*
- *"LPS Network uses the Suffolk County Council broadband. Smoothwall filtering and firewall systems are in place and managed for us by School's Choice ICT and are accessible by the school to manage as well. All the Windows devices are protected by Microsoft Windows Defender, 'Sophos InterceptX' and 'Sophos Server Advance' protection systems (managed by the school via a web interface. Chromebooks have their own built in protection updated automatically by Google. The Chromebooks are managed by the school domain device manager which is administered by the school ICT support. The iPads deployed in the school are managed by Apple School Manager and Moysle Mobile Device Management. Data backups are provided by an overnight backup to RDX removable drive, the latest of which is removed and taken off site. Backup images of the domain controller and SIMs server are taken at weekends. The network is managed by internal ICT support". (Information provided by internal ICT support technician.)*
- *With the support of the DSL, 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*
- *Maintain up-to-date documentation of the school's online security and technical procedures.*
- *Work closely with the DSL to ensure they understand who the nominated contacts are, what they can do and what data access they have, as well as the implications of all existing services and changes to settings that you might request (for example: for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite).*

Subject Area Leads Key responsibilities:

- *Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and pupils alike*
- *Consider how the UKCIS framework Education for a Connected World 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 school.*

Computing Volunteers and contractors
Key responsibilities:

- *Read, understand, sign and adhere to an acceptable use policy Appendix D*

- *Report any concerns, no matter how small, to the DSL as named in the Acceptable Use Policies*
- *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*

Pupils Key responsibilities:

- *Read, understand, sign and adhere to the pupil acceptable use policy and review this annually*
- *Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen*
- *Understand the importance of reporting abuse, misuse or access to inappropriate materials*
- *Know what action to take if they or someone they know feels worried or vulnerable when using online technology*
- *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 as 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 Key responsibilities:

- *Read, sign and promote the school's Parental Home-School Contract and Parental Acceptable Use Policy*
- *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 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 during any period of isolation/quarantine or bubble/school closure and flag any concerns*
- *Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible*
- *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.*

3. Education and curriculum

The following subjects have the clearest online safety links:

- *PSHE including Relationships education and health education.*
- *Computing*

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology, 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.

At our school, we recognise that online safety and broader digital resilience must be thread throughout the

curriculum and that is why we are working to adopt the cross-curricular framework 'Keychain Computing' and 'Project Evolve'

- Self-image & identity
- Online relationships
- Online reputation
- Copy right
- Ownership
- Online bullying
- Managing online information
- Health, well-being and lifestyle
- Privacy and security

4. Handling online safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and PSHE. General concerns must be handled in the same way as any other safeguarding concern.
School procedures for dealing with online-safety is detailed in the Child Protection & Safeguarding policy as well as the Behaviour & Anti-Bullying Policy. This school commits to take all reasonable precautions to ensure online safety,
but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school or during extended periods away from school. All members
of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to DSL on the same day. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case
the complainant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).
Staff may also use the NSPCC Whistleblowing Helpline.
The school will actively seek support from other agencies, as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour, which we consider is particularly disturbing or breaks the law.

For specific online safety concerns refer to the Child Protection and Safeguarding policy (Sexting, upskirting, bullying, sexual violence and harassment).
Misuse of school technology (devices, systems, networks or platforms)
Clear and well-communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and
outside of school). These are defined in the relevant Acceptable Use Policy as well as in this document. Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto
school property.

5. Social Media incidents

We have clear rules and expectations of behaviour for children and adults when using social media in our school community.
Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).
Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, we will request that the post be deleted and will expect this to be actioned

promptly. Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline (run by the UK Safer Internet Centre) for support or help to accelerate this process.

6. Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. Rigorous controls on the network, 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: 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 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

7. Appropriate filtering and monitoring

KCSIE 2020 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."

At our schools we have physical monitoring which means that children are always supervised by adults at all times.
At home, school devices are filtered and monitored when on home wifi connections.

8. Electronic communications - Email

Staff at this school use the GMail system for all school emails
This system is fully auditable, trackable and managed by LGfL on
behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- The chat function of Google Classroom (including Google Hangouts and Google Meet along with Zoom), are the only means of electronic communication to be used between staff and pupils(in both directions). Use of a different platform must be approved in advance by the headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- The Office Email address is the only means of electronic communication to be used between staff and parents (in both directions) and under no circumstances should private email addresses be used. Use of a different platform must be approved in advance by the Headteacher in advance.
- Staff or pupil personal data should never be sent/shared/stored on email. If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGf and if this is not possible then information should be password protected. Internally, staff should use the school network, including when working from home when remote access is available via the RAV3 system and G Suite.
- Currently we discourage children from emailing each other within the school or we do not allow children to email external accounts using a school-based email address. This system is closely monitored.

- *Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school into disrepute or compromise the professionalism of staff.*

Staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.

9. School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated who has the day-to-day responsibility of updating the content of the website. The site is managed by / hosted by Cygnet. The DfE has determined information which must be available on a school website.
Where other staff submit information for the website, they are asked to remember:

- *School have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.*
- *Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).*

10. Cloud platforms

We recognise the benefits of cloud computing platforms to enhance teaching and learning and ability to save and access our files. All staff have access to a Google Mail account and are able to use the applications provided by the
Google for Education's G Suite including the myDrive. We are now in a transitional period where our teaching staff are using myDrive to store and share school-based documents.
When using a cloud platform we adhere to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'.
For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The
Senior Leadership Team analyse and document systems and procedures before they are implemented, and regularly review them.

11. Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose and for how long. Parents/carers answer as follows:

- *For their child's photograph/video to be taken*
- *For displays around the school*
- *For social media*
- *For external use including: school website, paper-based school marketing and the newsletter*
- *For use on Google Classroom/Google Site*

Class teachers have up-to-date lists of which children have permission to have photos or videos taken. These can be checked at any time on SIMS. Any pupils shown in public facing materials are never identified with more than first
name (and photo file names/tags do not include full names to avoid accidentally sharing them). We aim for no members of staff to use their personal phone to capture photos or videos of pupils. However on occasion (with permission of SLT) the use of personal phones to capture photos or videos of pupils can take place if the following procedures are applied: appropriately linked to school activities; taken without secrecy and not in a one-to-one situation; always moved to school storage as soon as possible and after which they are deleted from personal devices or cloud services.

Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
Staff and parents are reminded annually (a signed declaration by parents with the Home- School Contract) about the importance of not sharing without permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

12. Social Media

Staff, pupils' and parents Social Media presence
Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies, which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermine staff morale and the reputation of the school.

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.
However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.
Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The school has an official Facebook page and requests that parents/carers do not to use this channel to communicate about their children.
Pupils are not allowed to be 'friends' with or make a friend request to any staff, governors, volunteers and contractors or otherwise communicate via social media.
Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) and this highlights the need for staff to remain professional in their private lives. In the reverse situation, however, staff must not follow such public student accounts.
Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute. We have an Online Communication (including Social Media) Code of Conduct for Staff Working with Children which all staff sign,

13. Extremism

The school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty (see CP & Safeguarding Policy). Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature by the school. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

14. Device usage

All staff with access to school devices are reminded about rules on the misuse of school technology including when devices are used at home which should be used as if they were in full view of a teacher or colleague.

Personal devices including wearable technology and mobile telephones

Year 5 and 6 Pupils, who walk to or from school alone, are allowed to bring mobile phones in to school.
Mobile phones have to be turned off before arrival on school property and not turned back on until the pupil has left the school premises. Upon arrival in the classroom, pupils should hand in their mobile phone to their class teacher who will keep them in an allocated space until the end of the school day.

At LCPS all staff who work directly with children should leave their mobile phones on silent and only use them when they not teaching. Child/staff data should never be downloaded onto a private phone.
Volunteers, contractors, governors should keep their phones away and on silence during school hours. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission should be sought from the site team or a member of SLT and this should be done in the presence of a member staff during school hours.

Parents are asked to be respectful when using their mobile phones on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children.

Network/internet access on school devices

Pupils are not allowed networked file access via personal devices.
Home devices are issued to some pupils. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked. The devices are filtered monitored when on home wifi connections.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours unless in an emergency.
Staff and Parents have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be able to use their personal mobile phone in an emergency or in any other communication with the school. Support staff and volunteers should not be using their mobile phones at any other time unless authorised by the teacher leading the trip.
In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains undesirable material, including but not exclusive to sexual images, violence or bullying.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other

devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Appendix A
Acceptable Use Agreement (pupils KS1)

Name of pupil:

Date:

Class:

This is how I KEEP SAFE online:

I follow the digital 5 a day
I only use the devices or apps, sites or games I am allowed to
I check before I use new sites, games or apps by a trusted adult
I ask for help if I am stuck or not sure
I tell a trusted adult if I am upset, worried, scared or confused
If I get a funny feeling in my tummy, I talk to an adult
I look out for my friends and tell someone if they need help
I know people online are not always who they say they are
I think before I click
I do not keep secrets or do dares and challenges just because someone tells me to
I keep my body to myself online
I do not share private information
I am kind and polite to everyone

My trusted adults are:

At school: _____ _____

At home: _____ _____

Appendix B
Acceptable Use Agreement (pupils KS2)

Name of pupil:

Date:

Class:

This is how I KEEP SAFE online:

I will remember to follow the digital 5 a day (Stay connected, Be active, Get creative, Give to others and Be mindful)
I use the school's internet and devices for schoolwork and other activities to learn and have fun
I learn at home even when I cannot be at school due to Covid
At home or school, I only use the devices, apps sites and games I am given permission to use from a trusted adult or they are present being present
I only use sites, games and apps that my trusted adults say I can
I won't share anything that I know another person wouldn't want shared, or which might upset them.
I keep my passwords to myself and ask for them to be reset if anyone finds them out.
I think before I click on links or share so that I am careful to protect my online reputation
I understand that some people might not be who they say they are
I do not share private information
I keep my body to myself online
I don't send any photos without checking with a trusted adult
I ask for talk to a trusted adult if I am upset, worried, scared or unsure about
I know that some apps, games, websites and social networks have age restrictions and rules on how to behave and I respect this
I am considerate, respectful and kind online
I keep others safe by talking to a trusted adult if I am worried about something I see or hear
I will not meet with anyone I speak to online that I do not know in real life
I can say no online if I need to and do not have to do something just because a 'friend' asks me too.
I will ask permission to do live video streams on my own

My trusted adults are:

At school: _____ _____

At home: _____ _____

Appendix C
Acceptable Use Agreement – Staff, Governors and Volunteers

Name of Staff Member/Governor (Volunteer or Visitor):

Date:

I have read and understood the school's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.

I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher.

During remote learning I will follow the school's Remote Learning Policy

I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the PSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.

I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

- *not sharing other's images or details without permission*
- *refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.*

I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.

Details on social media behaviour, the general capture of digital images/video and on my use of personal devices is stated in the full Online Safety policy. If I am not sure if I am allowed to do something in or related to school, I will not do it.

I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.

I agree to adhere to all provisions of the school Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Headteacher if I suspect a breach. I will only use complex passwords and not use the same password as for other systems.

I will not store school-related data on personal devices, storage or cloud platforms. USB keys, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.

I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature by the school.

I understand and support the commitments made by pupils, parents and fellow staff, governors and volunteers in their Acceptable Use Policies and will report any infringements in line with school procedures.

I will follow the guidance in the safeguarding and online-safety policies for reporting incident.

I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

The school may exercise its right to monitor the use of the information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system is being used for criminal purposes or storage of inappropriate or unlawful text, imagery or sound.
I have read, understood and accept the Staff ICT Acceptable Use Policy.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix D
Acceptable Use Agreement – Visitors & Contractors

Name of Visitor or Contractor:

I am agreeing to:

I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's systems security, monitoring and filtering systems and/or viewed by an appropriate member of staff.

I 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.

I will leave my phone in my pocket and place it on silent. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff.

If I am given access to school-owned devices, networks, cloud platforms or other technology:

- *I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use*
- *I will not attempt to access any pupil / staff / general school data unless expressly instructed to do so as part of my role*
- *I will not attempt to make contact with any pupils or to gain any contact details under any circumstances*
- *I will protect my username/password and notify the school of any concerns*
- *I will abide by the terms of the school Data Protection Policy and GDPR protections*

I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.

I will not reveal any new information on social media or in private which shows the school in a bad light or could be perceived to do so.

I will not do or say anything to undermine the positive online-safety messages that the school disseminates to pupils and will not give any advice on online-safety issues unless this is the purpose of my visit and this is pre-agreed by the school.

I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult).

I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view material which is or could be perceived to be inappropriate for children or an educational setting

To be completed by the visitor/contractor:
I have read, understood and agreed to this policy.

Signature/s: _____

Name: _____

Organisation: _____

Visiting/accompanied by: _____

Date/ time: _____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: _____

Name / role / date / time: _____

Appendix E
Acceptable Use Agreement – Parents & Carers

Name of Parent or Carer:

I am agreeing to:

I understand that my child school uses technology as part of the daily life of the school when it is appropriate to support teaching and learning and the smooth running of the school, and to help prepare the children in our care for their future lives.

I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering. However, the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, which can sometimes be upsetting.

I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring. These should be used in the same manner as when in school, including during any remote learning periods.

I will promote positive online safety and model safe, responsible and positive behaviours in my 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.

The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

I will follow the school's digital images and video policy, which outlines when I can capture and/or share images/videos. I will not share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes and it will only do so publicly if I have given my consent.

I understand that for my child to grow up safe online, s/he will need positive input from school and home, so I will talk to my child about online safety.

I understand that my child needs a safe and appropriate place to do remote learning if school or bubbles are closed (similar to regular online homework). When on any video calls with school, it would be better not to be in a bedroom but where this is unavoidable, my child will be fully dressed and not in bed, and the camera angle will point away from beds/bedding/personal information etc. Where it is possible to blur or change the background, I will help my child to do so.

If my child has online tuition, I will undertake necessary checks where I have arranged this privately to ensure they are registered/safe and reliable, and for any tuition remain in the room where possible, and ensure my child knows that tutors should not arrange new sessions or online chats directly with them.

I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. (Internet Matters provides guides to help parents do this easily for all the main internet service providers in the UK).

I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day: childrenscommissioner.gov.uk/our-work/digital/5-a-day/

I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed, and I understand that s/he will be subject to the school's Behaviour Policy if s/he does not follow these rules.

You can talk to your child's class teacher or a member of the Senior Leadership Team if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/we have read, understood and agreed to this policy.

Signature/s: _____

Name/s of parent / guardian: _____

Parent / guardian of: _____ ***Date:*** _____

Appendix F
Online Communication (including Social Media) Code of Conduct for Staff

Working with Children

Why do we need a code of conduct for communication?

Over the past years the use of social networking sites, such as X and Facebook has become increasingly popular. Such sites are used to chat with and share information, photographs and news with friends across the world.

The use of these sites has many benefits. However, there are potential problems concerning privacy and inappropriate usage. These may include breaches of confidentiality, unsuitable language or images, and in some cases breaches of the law.

Examples of such problematic usage of social networking could be:

- *Staff referring to parents or children by name*
- *Staff referring to forthcoming trips/visits*
- *Staff using derogatory or offensive language about parents, colleagues, managers, or the organisation for which they work.*
- *Staff posting images of themselves in inappropriate dress or situations*
- *Staff posting images of pupils on the internet*
- *Staff participating in illegal activities such as the sharing of indecent images of children*
- *Partners or friends posting inappropriate comments concerning staff*
- *Partners and friends posting images that show staff members in situations which may not be in keeping with their professional status*

What are we protecting?

- *Ourselves as members of staff: our privacy, reputation and safety*
- *The children we work with: their privacy, reputation and safety*
- *The reputation of our employer*

This code of conduct is designed to protect all staff who use such sites in their private lives.
As adults who work with children, we have a duty to demonstrate the highest standards of conduct or integrity. We need to ensure that our actions in our private lives do not put us into situations where our conduct or integrity might be called into question or potentially bring our employer into disrepute.
This could result in disciplinary action by your employer or even criminal prosecution. This code of conduct sets out expectations around your online behaviour that could affect professional standing, integrity and dignity.

Code of conduct:

- *Staff should not enter into online contact with children (regardless of age) they work with, parents or their families. Friend requests from parents or children under the age of 18 (past or present) in this context should be politely declined by explaining that it is against school policy, which is designed to protect staff from abuse and misunderstandings. Exceptions may be made by the Headteacher for pre-existing friends/ family links. No children under the recommended age of social media accounts should be added regardless of links.*
- *Staff should not create web pages, groups or contact lists concerning professional activities carried out on behalf of the school unless they have express written permission from a senior manager.*
- *Only make contact with children for professional reasons and in accordance with any organisational policy.*
- *There must be absolutely no private online contact between staff and any children with whom they have a work-related relationship.*
- *Staff should not store images or videos of any children with whom they have a work-related relationship, on their private machines.*
- *Staff should not post images or videos of pupils, with whom they have a work-related relationship, on any social networking site/the internet.*

- *Online contact made as part of professional duties should always be carried out using technologies provided by the school or local authority. These technologies should have the capability of logging and storing records securely.*
- *Avoid, where possible, sending emails to staff after 6pm. Any emails sent after 6pm are upon agreement with individuals or as an urgent/necessary communication for the following day. Staff should not feel obligated to reply to emails after their working hours. 'Reply all' emails should be avoided unless it's necessary for* ***all staff*** *to see the response. This is to support work/life balance and well-being of staff.*
- *Staff are strongly advised to be careful about what they say online in contact with other young people such as relatives or family friends. This applies to any media, for example: images, audio or video material.*
- *Any contact with children and young persons after they have left the organisation (e.g. moved to a secondary school) should be sanctioned by a senior manager within the organisation and the parent and not occur through social networking sites or other online communication technologies.*
- *Do not give personal contact details to children including their mobile telephone number and details of any blogs or personal websites.*
- *Not use internet or web-based communication channels to send personal messages to a child.*
- *Ensure that if staff use a social networking site, details are not shared with children and privacy settings are set at maximum.*
- *School should not be named or referred to on any social media posts without the consent of SLT. Any social media posts regarding school should be made using the school account. E.g. Requests in the community for resources etc.*

This code does not cover:

- *Social contact between colleagues. However, staff need to be mindful of what they are posting and who can see it. This is important in respect of confidentiality, workplace relationships. Online contacts may not appreciate the difference between private and professional comments.*
- *Membership of professional networks or forums: these are usually covered by a professional body's own code of conduct.*
- *Membership of forums, although in extreme cases legal restrictions may apply. Staff should however remember that what they say may reflect upon their professional lives and moderate their comments accordingly.*

Staff privacy and dignity:

- *Staff are strongly recommended to check that their online privacy settings only allow "friends" to see their profiles.*
- *Staff are advised not to accept friend requests from people who are not personally known to them.*
- *Staff should ask colleagues before photographs are posted which may cause them embarrassment. Staff posting their own images should bear in mind the fact that any image can easily be downloaded and manipulated and they should choose which images they share accordingly.*
- *It is recommended that staff do not post images that could be used to identify their homes or families.*
- *All staff are advised to make themselves familiar with the parent/carer pages on the CEOP "Think You Know" site at www.thinkyouknow.co.uk and keep themselves up to date with the risks of emerging technologies.*

Name: .....

Signed: .....

Date: .....

Appendix G
Electronic Device Acceptable Use Policy

The policies, procedures and information within this document applies to all iPads, Chromebooks or any other IT handheld device used in the classroom or around the school site. Teachers and other school staff may also set additional requirements for monitoring and managing use within their own classroom.

Responsibilities – class teachers/support staff/pupils:

- *Protective covers/cases must be used on all iPads.*
- *The iPad and Chromebooks screen is made of glass and therefore is subject to cracking and breaking if misused: never drop nor place heavy objects (books, laptops, etc.) on top of the iPad. The class teacher is responsible for ensuring that pupils use the equipment correctly.*
- *Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.*
- *The devices must not be left unattended at any time.*
- *The class teacher/adult in charge of the class is responsible for ensuring that the devices are stored away safely and securely after use in the appropriate storage trolley and to check that all devices removed from the secure trolley are returned at the end of the session.*
- *Class teacher iPad minis must be stored securely in either the safe provided in the classroom or a lockable cupboard.*
- *A termly check will be made on the equipment by the Computing Lead/ office staff.*

Safeguarding and Maintaining as an Academic Tool:

- *Syncing the iPads to iTunes or iCloud will be maintained by a School Administrator as will updating the Chromebooks.*
- *The class teacher is responsible for any photos taken on the iPads or Chromebooks and that these are subject to our GDPR policies and procedures.*
- *Pupils should not use the devices to take photos unless it is part of the lesson and the class teacher should ensure that these are deleted at the end of the lesson.*
- *It is the responsibility of the class teacher(s) to ensure that the devices are checked on at least a half-termly basis to ensure that all photos have been erased.*
- *Random checks on the devices to ensure photos are deleted will be made by the Computing Lead and the SBM during their GDPR checks.*
- *All devices are subject to routine monitoring by the Computing Lead or other member of the SLT.*
- *All devices must be used within the guidelines and procedures of the schools Online Safety Policy and Acceptable Use of the Internet agreements. Any breach of the policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal or inappropriate activity.*
- *All pupils have individual pupil Google Chrome accounts which can be used to log in and out of their Chromebooks each time.*
- *The devices should not be taken out of school at any time.*
- *The whereabouts of the devices should be known at all times. An Inventory is kept of all the devices, serial numbers and their locations electronically on the school's secure asset management system. If the location of an item(s) is to be changed then the School Business Manager should be notified first.*

Suspected loss or theft of device:

- *If a device cannot be located this MUST be notified to the Headteacher immediately in order for appropriate action to be taken which, dependent on circumstances, may include the requirement to report a breach to the Information Commissioner's Office under the GDPR regulations.*

Name: ……Signed: ……Date: ……