

Chacewater School




Online Safety Policy

Ratified Date: January 2024

Review Date: January 2025

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	DSL: Emma Law Deputy DSL: David Hick
	Online-safety lead (if different)	Emma Law
	Online-safety / safeguarding link governor	Polly Langford
	PSHE/RSHE lead	Emma Law
	Network manager / other technical support	TPAT IT Support- Ben White
	Date this policy was reviewed and by whom	David Hick - January 2024
	Date of next review and by whom	January 2025 - Governors

What's different about this policy for September 2023?

This year, there are changes to reflect trends we have seen over the past year and especially in the light of changes to KCSIE – the most significant change relating to filtering and monitoring, as well as to shorten this document.

The DSL has now been asked to take lead responsibility for webfiltering and monitoring, marking a clear shift. Schools now need to follow the new DfE standards and consider the roles and responsibilities of all staff – for DSLs and SLT, the challenge is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams. All staff need to be aware of the changes and renewed emphasis and play their part in feeding back about overblocking or gaps in the filtering provision. Schools will also be reviewing their approaches to monitoring in line with the standards (note that filtering and monitoring are not the same – there is guidance around this for DSLs at <https://safefiltering.lgfl.net>).

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' 2023 (KCSIE), 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside or be integrated into your school's statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we will involve staff, governors, pupils and parents in writing and reviewing the policy and make sure the policy makes sense and it is possible to follow it in all respects. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice.

Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Our aim is for this policy to be a continual working document so that it is updated regularly in line with guidance and the latest developments in the online world.

Who is in charge of online safety?

KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL can delegate activities but not the responsibility for this area and whilst subject leads, e.g. for RSHE will plan the curriculum for their area, it is important that this ties into a whole-school approach.

What are the main online safety risks today?

Current Online Safeguarding Trends

In our school over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Inappropriate use of messaging (e.g. Whatsapp), Snapchat, TikTok and generating/sharing images without consent.
- Inappropriate content viewed on YouTube, including their links to hate crimes and harmful content, including pornography
- Increased screen time at home
- Inappropriate use of Apps and Games, both relating to their age rating and the amount of time spent on these games.

Nationally, some of the latest trends of the past twelve months are outlined below. These should be reflected in this policy and the acceptable use agreements we use, and seen in the context of the 5 Cs (see KCSIE for more details), a whole-school contextual safeguarding approach that incorporates policy and practice for curriculum, safeguarding and technical teams.

We may be updating this policy during the year to reflect any changes resulting from the Online Safety Bill being passed into law.

Self-generative artificial intelligence has been a significant change, with students having often unfettered access to tools that generate text and images at home or in school. These tools not only represent a challenge in terms of accuracy when young people are genuinely looking for information, but also in terms of plagiarism for teachers and above all safety: none of the mainstream tools have end-user safety settings, most have an age limit of 13 or even 18 and in spite of basic rude words not delivering results, will easily produce inappropriate material. Schools not only need to tackle this in terms of what comes into school but also educating young people and their parents on use of these tools in the home.

The continued **cost-of-living crisis** has meant that children have spent more time online and therefore exposed to all manner of online harms as families have had to cut back on leisure activities and the public provision of free activities for young people has reduced further.

Against this background, the Ofcom 'Children and parents: media use and attitudes report 2023' has shown that **YouTube** remains the most used site or app among all under 18s and the reach of **WhatsApp, TikTok and Snapchat** increased yet further. As a school we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore remember to remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 20% of 3-4 year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3 to 6 year olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7-10 year old age group is the fastest growing for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023

Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed the ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography. This has coincided with the rise of misogynistic influencers such as Andrew Tate, which had a significant influence on many young boys over the past year which schools have had to counter.

From the many schools that LGfL spoke to over the past year, there was a marked increase in the number of schools having issues with fights being filmed and shared, a disturbing increase in the cases of self-harm and sexual abuse being coerced with threats of violence (many even in primary schools).

There has been a significant increase in the number of fake profiles causing issues in schools, both for schools – where the school logo and/or name have been used to share inappropriate content about students and also spread defamatory allegations about staff, and also for students, including where these are used to bully others (sometimes even pretending to be one student to bully a second student).

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff shared drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

Overview

Aims

This policy aims to:

- Set out expectations for all Chacewater School's 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 Relationships and Positive Behaviour Policy or Anti-Bullying Policy).
- Understanding the need to not criminalise the behaviours outlined in this policy, but to educate and ensure victim blaming does not become prevalent as a result.
- Providing opportunities for parents to feedback, raise concerns and attend relevant forums to share and learn.

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Child Protection & Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MARU) and normally the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, [reportingsgfl.net](https://www.reportingsgfl.net) has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people. Training is also available via [safetraining.sgfl.net](https://www.safetraining.sgfl.net)

Scope

This policy applies to all members of Chacewater School's 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.

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.

In 2023/2024, it is vital that all members understand their responsibilities and those of others when it comes to filtering and monitoring. All staff have a key role to play in feeding back on potential issues.

See Appendix for a breakdown of roles and responsibilities.

Education and curriculum

It is important that schools establish a carefully sequenced curriculum for online safety that builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, [Teaching Online Safety in Schools](#) recommends embedding teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils – dedicated training around this with curriculum mapping for RSHE/PSHE and online safety leads is available at [safetraining.lgfl.net](#)

RSHE guidance also recommends schools assess teaching to “identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress.” [safeskillsinfo.lgfl.net](#)

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place). *“Parents and carers are likely to find it helpful to understand what systems schools use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online” (KCSIE 2023).*

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. disinformation, misinformation and fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Chacewater 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 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for pupils with SEND) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership. Curriculum plans will be found on the School Website.

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, PSHE/RSHE and Citizenship). It is also important to note that parents - and often professionals - often feel unable to help/support children because they do not consider themselves 'experts' in technology. Parents and professionals do have the skillset to respond to online safety issues, as these are the same skills that they would respond to any form of harm.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online safety will be mostly detailed in the following policies (primarily in the first key document):

- CAPH Safeguarding and Child Protection Policy
- Child-on-Child Abuse Policy
- Anti-Bullying Policy
- Relationship (Positive Behaviour) Policy
- Acceptable Use Policies
- Prevent Risk Assessment & Policy
- TPAT Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Low Level Concern Policy

Chacewater School commits to take all reasonable precautions to ensure safeguarding pupils online, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact 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 the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline (you may want to display a poster with details of this / other helplines in the staff room – see [posters.lgfl.net](https://www.lgfl.net/posters) and [reporting.lgfl.net](https://www.lgfl.net/reporting)).

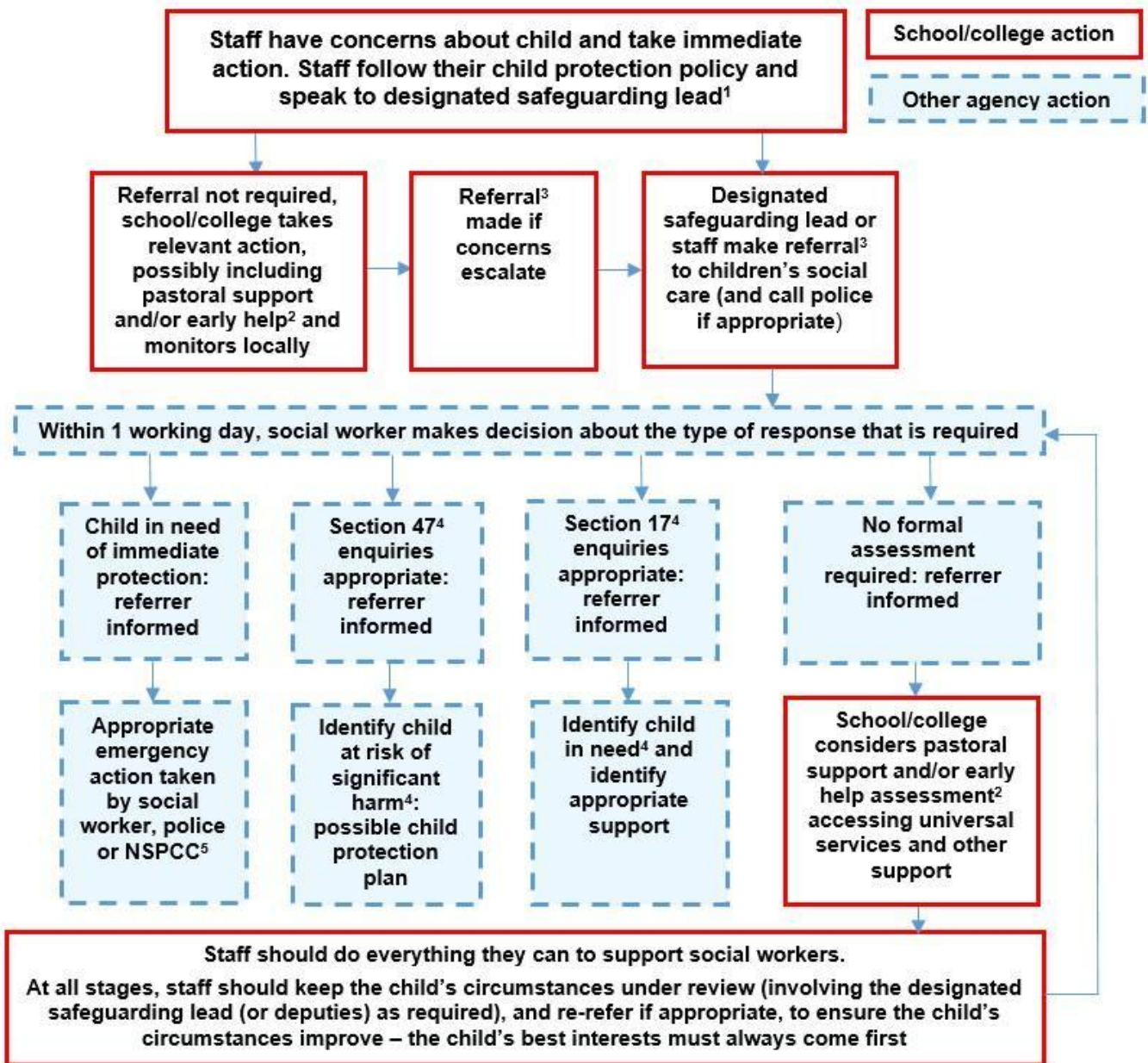
The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance [Behaviour in Schools, advice for headteachers and school staff](#) September 2022 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 32-34 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

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 concerning or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

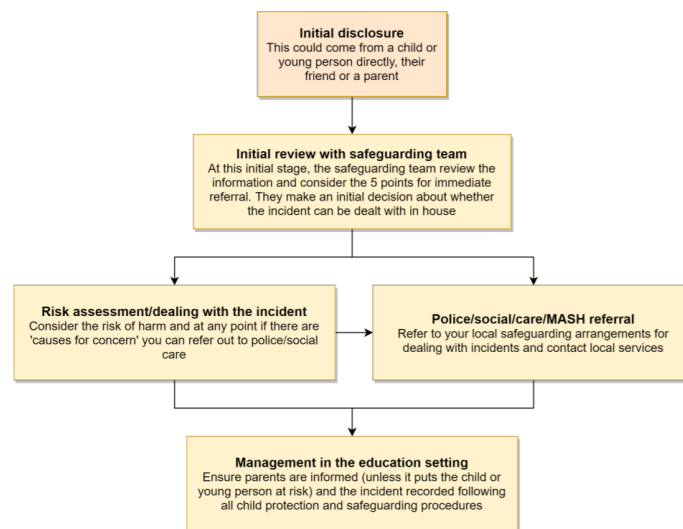


Sexting – sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as [Sharing nudes and semi-nudes: advice for education settings](#) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sharing nudes and semi-nudes: how to respond to an incident](#) for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

The school DSL will in turn use the full guidance document, [Sharing nudes and semi-nudes – advice for educational settings](#) to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in

Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

It is important to be aware that in the past 12 months there has been an increase in anecdotal reports of fights being filmed and fake profiles being used to bully children in the name of others. When considering bullying, staff will be reminded of these issues.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Child-on-child sexual violence and harassment

Part 5 of Keeping Children Safe in Education covers 'Child-on-child sexual violence and sexual harassment' and it would be useful for all staff to be aware of many aspects outlined there to support a whole-school response; case studies are also helpful for training.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour. Other behaviours relating to image sharing are also on the rise, and must be monitored carefully and responded to appropriately.

Grooming - Sexual Abuse

Keeping Children Safe in Education makes it explicit that 'grooming' is a key act in Sexual Abuse, Child Sexual Exploitation, Sexual Violence and Sexual harassment. Grooming can happen online and is where someone befriends a child and builds up trust with the intention of exploiting them and causing harm. This can include exploitation to obtain sexually explicit images and videos of the child. It is important that staff recognise the signs and children are taught about 'red flags' in chats which are important to report, block and inform a trusted adult.

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, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

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 and handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/closure/quarantine etc.

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.

The new responsibilities for filtering and monitoring, led by the DSL and following the new DfE standards, may mean that more such incidents will be discovered in the coming year but the school will do its best to remind pupils and staff of this increased scrutiny at the start of the year.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Chacewater School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school's Relationships and Positive Behaviour Policy 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, the school 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, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cybersecurity policy which can be found on TPAT website. It is important to remember that there is a close relationship between both data protection and cybersecurity and a school's ability to effectively safeguard children. Schools are reminded of this in KCSIE which also refers to the DfE Standards of Cybersecurity for the first time in 2023.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

Appropriate filtering and monitoring

Keeping Children Safe in Education has long asked schools to ensure "appropriate" webfiltering and monitoring systems which keep children safe online but do not "overblock".

Since KCSIE 2023, in recognition of the importance of these systems to keeping children safe, the designated safeguarding lead now has lead responsibility for filtering and monitoring (see page 1 for the DSL name and the named governor with responsibility for filtering and monitoring).

Schools are also asked to follow the new DfE filtering and monitoring standards, which require them to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs

As schools get to grips with these new standards, the challenge for DSLs and SLT is to better understand, review and drive the rationale behind decisions in this area. Tech teams and safeguarding teams will need to work much more closely together for this to be possible and technicians will be charged to carry out regular checks and feed back to DSL teams.

ALL STAFF need to be aware of the changes and renewed emphasis and play their part in feeding back about areas of concern, potential for students to bypass systems and any potential overblocking. They can submit concerns at any point via CPOMS and will be asked for feedback at the time of the regular checks which will now take place.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding as well as via AUPs and regular training reminders in the light of the annual review and regular checks that will be carried out.

It is very important that schools understand the difference between filtering and monitoring, the meaning of overblocking and other terms, as well as how to get the best out of systems. There are guidance videos and flyers to help with this at <https://safefiltering.lgfl.net> and training is provided for all staff / safeguarding teams / technical teams as appropriate.

At Chacewater School:

- web filtering is provided by SWGFL and JAMP for school devices used in the home
- changes can be made by TPAT IT Support
- overall responsibility is held by the DSL with further SLT support

- technical support and advice, setup and configuration are from TPAT
- regular checks are made half termly by Emma Law and David Hick to ensure filtering is still active and functioning everywhere.
- an annual review is carried out as part of the online safety audit to ensure a whole school approach” template onlinesafetyaudit.lgfl.net]

According to the DfE standards, “a variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through OnGuard monitoring software

Chacewater Primary School currently receives support through TPAT IT Support.

Messaging/commenting systems (incl. email, learning platforms & more)

Authorised Systems:

- Pupils at Chacewater School communicate with each other and with staff using Google Platforms, Natterhub and Showbie.
- Staff at this school use the email system provided by TPAT IT Services for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system. Staff are permitted to use this email system to communicate with colleagues and external agencies. School staff are permitted to contact parents using this platform, however parents can only contact chacewater@tpacademytrust.org or the designated class email addresses e.g. bueroak@chacewater.tpacademytrust.org
- School staff will also use parent pay and Arbor to communicate with parents.

Any systems above are centrally managed and administered by the school or authorised IT partner (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation.

Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.

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).

Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / usage principles

- More detail for all the points below are given in the Social media section of this policy as well as the school's acceptable use agreements, behaviour policy and staff code of conduct.
- 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 (for staff) might bring the school into disrepute or compromise the professionalism of staff.
- Data protection principles will be followed at all times when it comes to all school communications, in line with TPAT Data Protection Policy and only using the authorised systems mentioned above.
- 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 (and will be dealt with according to the appropriate policy and procedure).

Online storage or learning platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc.

For all these, it is important to consider data protection and cybersecurity before adopting such a platform or service and at all times when using it. Chacewater School has a clear cybersecurity and data protection policy which staff, governors and volunteers must follow at all times.

Ensure these are covered in those documents and training: password hygiene, cybersecurity and data protection best practice, privacy statements, collaboration with your DPO, file sharing permissions and procedures, use of two-factor authentication, parental permissions, where pupil work can be displayed, the differences between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

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 site is managed by / hosted by Eschools.

The DfE has determined information which must be available on a school website, this is checked regularly to ensure compliance.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected. If in doubt, check with TPAT.

Cloud platforms

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 following principles apply:

- Privacy statements inform parents and children (13+) when and what sort of data is stored in the cloud
- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student 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 (beyond internal assessment, which does not require express consent) and for how long. Parents answer related to use on the following:

- For official school purposes of promoting or publicising school events e.g. newsletter
- For use on the school website
- For use in video recordings to promote the school
- For use in the school’s own records, archives and future interest e.g. photographs of sports teams
- Consent that children can appear in video recordings or in collections of photographs stored on CD roms.
- Consent to be included in any images taken by other parents or carers who wish to photograph or record school events
- For use by the press

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose.

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).

All staff are governed by their contract of employment and the school’s Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are

stored. At Chacewater School members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Photos are stored on the school network or on Eschools in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

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 children

Pupils are advised to be very careful about placing any personal photos on social media. 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. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social media

Chacewater's SM presence

Chacewater School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

David Hick and the office staff are responsible for managing our Twitter and Facebook accounts.

Staff, pupils' and parents' SM presence

Social media (including 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.

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 undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school has dealt with issues arising on social media involving pupils/students 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. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming year and that there is massive contention around age verification in national debate.

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/students 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 (you don't need to know them – ask your child to explain it to you), 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). You may wish to refer to the [Digital Family Agreement](#) to help establish shared expectations and the [Top Tips for Parents](#) poster along with relevant items and support available from parentsafe.lgfl.net and introduce the [Children's Commission Digital 5 A Day](#).

Although the school has an official Facebook & X-Twitter account and will respond to general enquiries about the school, it asks parents/carers not to use these channels, especially not to communicate about their children.

Email is the official electronic communication channel between parents and the school. Social media, including chat apps such as WhatsApp, are not appropriate for school use.

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/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account) as laid out in the AUPs. However, we

accept that this can be hard to control (but 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.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so 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).

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.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a significant number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital images and video and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils/students** are allowed to bring mobile phones in for emergency use only. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to parents being contacted and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **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. See also the Digital images and video section on page and Data protection and data security section on page. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf, ask for the message to be left with the school office or have their phone on them with the permission of the headteacher.

- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. 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 of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets when they are on site and know that taking pictures is not permitted. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Network / internet access on school devices

- **Pupils** are allowed to bring mobile phones in, bringing them in the front entrance in the mornings, leaving them in the office and picking them up on their exit through the entrance door at 3.15. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **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. See also the 'Digital images and video' section of this document and the school data protection cybersecurity policies. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office/Headteacher/Deputy Headteacher to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets/bags and turned off. 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 of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** When at school events, please refer to the Digital images and video section of this document.

Trips / events away from school

For school trips/events away from school, teachers will take their own mobile phone for use in case of an emergency. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools](#)', the Headteacher/Principal 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 – Roles and Responsibilities.

Please read the relevant roles & responsibilities section from the following pages.

All school staff must read the “All Staff” section as well as any other relevant to specialist roles

Roles:

- All Staff
- Headteacher/Principal
- Designated Safeguarding Lead
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE / RSHE Lead/s
- Computing Lead
- Subject / aspect leaders
- Network Manager/technician
- Data Protection Officer (DPO)
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All Staff

All staff should sign and follow the staff acceptable use policy in conjunction with this policy, the school’s main safeguarding policy, the code of conduct/handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes reporting any concerns, no matter how small, to the designated safety lead as named in the AUP, maintaining an awareness of current online safety issues (see the start of this document for issues in 2023) and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.

Staff should also be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about overblocking, gaps in provision or pupils bypassing protections.

Headteacher– David Hick

Key responsibilities:

- Foster a culture of safeguarding where online-safety is fully integrated into whole-school safeguarding
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE (including technology in use in the school).
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance
- Ensure ALL staff undergo safeguarding training (including online-safety) at induction and with regular updates and that they agree and adhere to policies and procedures
- Ensure ALL governors undergo safeguarding and child protection training and updates (including online-safety) to provide strategic challenge and oversight into policy and practice and that governors are regularly updated on the nature and effectiveness of the school’s arrangements.

- 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 remote systems are implemented according to child-safety first principles
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL— in particular understand what is blocked or allowed for whom, when, and how as per KCSIE
 - In 2023/4 this will involve starting regular checks and annual reviews, upskilling the DSL and appointing a filtering and monitoring governor
- 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
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- 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 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
- 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 the school website meets statutory requirements

Designated Safeguarding Lead / Online Safety Lead – Emma Law

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2021):

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead** responsibility should not be delegated”
- Work with the HT and technical staff to review protections for pupils in the home where possible and as a minimum to make parents aware of their responsibilities and need to monitor content and usage of any devices used in the home. and remote-learning procedures.
- 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 SENDCOs 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 procedures and technology, including that the same principles of online safety and behaviour apply

- Work with the headteacher, DPO 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 safeguarding and “undertake Prevent awareness training.” – see safetraining.lgfl.net and prevent.lgfl.net. Complete relevant training on the academy trust’s Safesmart system.
- 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.
- 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.
- 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.
- 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 also aware. Are you talking to your technical teams? 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).
- Ensure the updated [2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges](#) Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
 - all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages at kcsietranslate.lgfl.net
 - 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

Governing Body, led by Online Safety / Safeguarding Link Governor – Mrs Polly Langford

Key responsibilities (quotes are taken from Keeping Children Safe in Education)

- Key responsibilities (quotes are taken from Keeping Children Safe in Education)
- 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](#)
- Undergo (and signpost all other governors and Trustees to attend) safeguarding and child protection training (including online safety) at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.
- 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 coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Work with the DPO, DSL and headteacher to ensure a 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
- Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring
- “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.”

RHSE/PSHE Lead – Emma Law

Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from recent trends in self-generative artificial intelligence, financial extortion and sharing intimate pictures 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."

- Focus on the underpinning knowledge and behaviours outlined in [Teaching Online Safety in Schools](#) in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Assess teaching to "identify where pupils need extra support or intervention [through] tests, written assignments or self evaluations, to capture progress" to complement the computing curriculum,.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.
- Note that an RSHE policy should be included on the school website.
- 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

Computing Lead – Shelley Hoare (David Hick during maternity leave)

Key responsibilities:

- 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 RHSE lead 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 ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- 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 RHSE curriculum, 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/OSL 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 – TPAT IT Support – Ben White

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.
- Note that KCSIE changes expect a great understanding of technology and its role in safeguarding when it comes to filtering and monitoring and in 2023/4 you will be required to support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as now recommended in KCSIE. This should also include a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the new DfE standards, protections for pupils in the home and remote-learning.
- 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
- Work closely with the designated safeguarding lead / online safety lead / data protection officer/ RHSE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- 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
- Maintain up-to-date documentation of the school's online security and technical procedures
- 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.
- Ensure the data protection policy and cybersecurity policy are up to date, easy to follow and practicable
- 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 (DPO) – John Walker (TPAT)

Key responsibilities:

- Alongside those of other staff, provide data protection expertise and training and support the DP and cybersecurity policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools, 2023*, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children."
- Note that retention schedules for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead
- 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.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy ([See Appendix](#))

Parents/carers

Key responsibilities:


- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children 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.
-

External groups including PTA

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- 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

Appendix – Chacewater School Acceptable Use - Staff, Volunteers and Governors

	Name of school	Chacewater School
	AUP review date	September 2023
	Date of next review	September 2024
	Who reviewed this AUP?	E-safety team – David Hick, Emma Law and Shelley Hoare

Refers to the use of all digital technologies in school: i.e. **e-mail, internet, network resources, VLE (Eschools), software, communication tools, equipment and systems:**

- I will follow the Online Safety policy (including for mobile and handheld devices).
- I will only use the school’s digital technology resources and systems for professional purposes or for uses deemed ‘reasonable’ by the Head and Governing Body.
- I will not share my passwords to anyone.
- I will follow ‘good practice’ advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else’s password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / VLE(Eschools) / network or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school’s network / information security policy.
- I will use an encrypted/password protected memory storage device or online platform (GDrive) to store any school documents (Teachers)
- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use the school approved e-mail system(s) / *communication systems* for any school business, including communication with parents. This is: Outlook. I will only enter into communication regarding appropriate school business.
- I will only use the school's approved systems: *Eschools/Google classroom/class emails* to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach to the DSL.
- I will not download any software or resources from the internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not use my own personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the school approved system (*e.g iPads*).
- I will follow the school's policy on use of mobile phones / devices at school (see Online Safety Policy)
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely and appropriately, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption/password, and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's Designated Safeguarding Lead (Emma Law) or appropriate senior member of staff if I feel the behaviour of any child with regard to computing and E-safety may be a cause for concern. I will log this on CPOMs.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead (Emma Law) or appropriate senior member of staff at the school.
- I understand that all internet usage and network usage can be logged, and that this information can be made available *to the Head / Safeguarding Lead* on their request.
- *Staff that have a teaching role only:* I will embed the school's e-safety / digital literacy curriculum into my teaching .
- I understand that the staff 'Whatsapp' group is for staff wellbeing and general ad-hoc communications. I will not use this group to communicate any serious or confidential matters regarding individual staff or children.




FS & KS1 Pupil Acceptable Use Policy

Name: _____



In order to stay safe online, I agree to be **SMART with a heart** :

S	Safe	I will not share my passwords or use someone else's log in details. I will only use the internet when my adults say and are supervising me. I will only use the devices, apps, games and websites my adults say I am allowed to. Anything I do online can be shared and might stay online forever.	
M	Meet	I will not speak to people I don't know online. I do not change clothes or get undressed in front of a camera. I will not share my personal information online such as where I live or photos of me.	
A	Accepting	I will think carefully before I click on links, adverts, emails. Is it safe? If I am not sure, I will ask an adult.	
R	Reliable	I know not to trust everything or everyone online. Think: Is it true? If I am not sure, I will ask an adult.	
T	Tell	I will tell a trusted adult if me or my friends are upset, confused or worried about something online.	
♥		I will always be kind and polite to others online. My trusted adults are: _____ at school _____ at home	

To find out more in FS & KS1: https://www.thinkuknow.co.uk/4_7/4-5/





LKS2 Pupil Acceptable Use Policy



Name: _____

In order to stay safe online, I agree to be **SMART with a heart** :

S	Safe	<p>I will not share my passwords.</p> <p>I will not attempt to log in to other's accounts.</p> <p>I will only use the internet with permission and when supervised.</p> <p>I will only visit the apps, sites and games approved by school.</p> <p>I know anything I do online can be shared and might stay online forever.</p>
M	Meet	<p>I only communicate online with people I already know offline or that my trusted adults know about.</p> <p>I will not share personal information with people I meet online: e.g my location, phone number or photos of myself.</p> <p>I will never meet up with anyone I have only met online.</p> <p>I never pretend to be someone else online.</p> <p>I don't change clothes or get undressed in front of a camera.</p> <p>If I get asked anything that makes me worried, upset or just confused, I should say no, and tell a trusted adult.</p>
A	Accepting	<p>I will think carefully before I click on links and adverts or download email attachments and files.</p> <p>I am aware some websites have age restrictions and I will respect and follow these.</p> <p>Is it safe? If I am not sure, I will ask an adult.</p>
R	Reliable	<p>I know not to trust or believe everything I read online.</p> <p>Think: Is it reliable? If I am not sure, I will check with a trusted adult.</p>
T	Tell	<p>I will tell a trusted adult if something online makes me or someone I know upset, worried or confused.</p> <p>If I make a mistake online, I am honest and don't try to hide it.</p>
		<p>I will always be kind and respectful to others online.</p> <p>I will respect other people's words, work and pictures and only edit or delete them if I have their permission.</p> <p>I won't share or say things online that would upset others.</p> <p>I will help others if they are upset or worried about something online by reporting it either to a trusted adult or through Childline: 0800 1111</p>





UKS2 Pupil Acceptable Use Policy



Name: _____

In order to stay safe online, I agree to be **SMART with a heart** :

S	Safe	<p>I will not use personal devices in school e.g mobile phones, I will only use the internet when supervised by a trusted adult. I will only visit the apps, sites and games approved by school. I will not share my passwords or attempt to 'log in' to other's accounts. I will use a safe, child-friendly search engine to filter online content. I will not try to access inappropriate, harmful or offensive content online. I know that my teachers monitor my online activity. I know that anything I do online can be shared and might stay online forever, even if I delete it.</p>
M	Meet	<p>I only communicate online with people I already know offline or that my trusted adults know about. I will not share personal information with people I meet online: e.g my location, phone number or photos of myself. I don't change clothes or get undressed in front of a camera. I will never meet up with anyone I have only met online. I never pretend to be someone else online. If I get asked anything that makes me worried, upset or just confused, I should say no and tell a trusted adult.</p>
A	Accepting	<p>I will think carefully before I click on links and adverts or download any email attachments and files. I will respect and follow the age restrictions of websites or content. Is it safe? If I am not sure, I will ask an adult.</p>
R	Reliable	<p>I know not to trust or believe everything I read online. Think: Is it reliable? If I am not sure, I will check with a trusted adult.</p>
T	Tell	<p>I will tell a trusted adult if something online makes me or someone I know upset, worried or confused. I will report any unsuitable content I access. If I make a mistake online, I am honest and don't try to hide it.</p>
		<p>I will always be kind and respectful to others online. I will respect other people's own words, work and pictures and only edit or delete them if I have their permission, being mindful of copyright laws. I won't share or say things online that would upset others. I will help others if they are upset or worried about something online by reporting it either to a trusted adult or through Childline 0800 1111</p>

BE SMART ONLINE



S

SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.



M

MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

THINK
U
KNOW
CO.UK

A

ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.



R

RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.



T

TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk



BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.



Device loan agreement for pupils

1. This agreement is between:

- 1) Chacewater School (“the School”)
- 2) [] (“the parent” and “I”)

And governs the use and care of devices assigned to the parent’s child (the “Pupil”). This agreement covers the period from the date the device is issued through to the return date of the device to the School.

All issued equipment shall remain the sole property of the School and is governed by the School’s policies.

1. The School is lending the Pupil a laptop (“the equipment”) for the purpose of doing schoolwork during the COVID19 Lockdown, from home.
2. This agreement sets the conditions for taking a [Chacewater laptop (“the equipment”)] home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the Pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the Pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that the Pupil and I are responsible for the equipment at all times, whether on the School’s property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the Headteacher at School and I acknowledge that I am responsible for the reasonable costs requested by the School to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the School when requested from the School in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

If the equipment is damaged, lost or stolen, and your child is eligible for pupil premium, contact David Hick Headteacher.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don’t leave the device in a car or on show at home
- Don’t eat or drink around the device
- Don’t lend the device to siblings or friends
- Don’t leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the School monitors the Pupil’s activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Causing intentional damage to ICT facilities or materials
- Making any hardware or software changes to the equipment without authorisation from the School IT Department
- Using inappropriate or offensive language

I accept that the School will sanction the Pupil, in line with our behaviour/discipline policy, if the Pupil engages in any of the above **at any time**.

4. Personal use

I agree that the Pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Do not share the equipment among family or friends
- Ensure the antivirus software is up to date

If I need help doing any of the above, I will contact the TPAT Central ICT Team on the email itsupport@tpacademytrust.org or ring them on 01872 613289 (Phone support is available between 8:30am and 3:30pm, Monday to Friday).

6. Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so.

I will ensure the return of the equipment to the School if the Pupil no longer attends the School.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

DEVICE SERIAL NUMBER	
DEVICE MAKE / MODEL	
PUPIL'S FULL NAME	
PARENT'S FULL NAME	
PARENTS SIGNATURE	
DATE	