# Policy for

# Online Safety

**Contents**


1. **Introduction and Overview**
   - What is this policy?
   - Rationale and Scope
   - Roles and responsibilities
   - How the policy will be communicated to staff/pupils/community
   - Review and Monitoring

2. **Education and Curriculum**
   - Pupil Online Safety curriculum
   - Staff and governor training
   - Parents awareness and training
   - Expected conduct

3. **Handling online-safety concerns and incidents**
   - Actions where there are concerns about a child
   - Sexting – sharing nudes and semi-nudes
   - Upskirting
   - Bullying
   - Sexual violence and harassment
   - Misuse of school technology (devices, systems, networks or platforms)
   - Social media incidents
   - Extremism
   - Generative AI

4. **Managing the IT Infrastructure**
   - Network management (user access, backup, curriculum and admin)
   - Data protection and data security
   - Internet access, security (virus protection) and filtering

5. **Electronic communication**
   - Authorised systems
   - School website
   - Cloud Platforms
   - Digital images and video
   - Social Media

6. **Device Usage**
   - Personal mobile phones and devices
   - Digital images and video
   - Searching and confiscation
   - Asset disposal

7. ***Appendices***
   - *Acceptable Use Agreement (Staff/Governors/Volunteers)*
   - *Acceptable Use Agreement (KS2 Pupils)*
   - *Acceptable Use Agreement (KS1 Pupils)*
   - *Acceptable Use Agreement including photo/video permission (Parents)*
   - *Protocol for responding to Online safety incidents*

| | |
|---|---|
| **Governor Responsibility:** | Learning & Community Committee |
| **Staff Responsibility:** | Reviewed by R Binger |
| **Review Period:** | Bi-annual |
| **Status:** | Non-statutory |
| **Reviewed:** | Spring 2025 |
| **Next Review Date:** | Spring 2027 |
| **Computing Governor:** | Amir Gold |

# 1. INTRODUCTION AND OVERVIEW

## 1.1 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' 2024 (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 the 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.

## 1.2 Aims

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Tetherdown school community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Helping safeguarding and senior leadership teams to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. RSHE) and beyond.
- Helping 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, regardless of device or platform and that the same standards of behaviour apply online and offline.
- Facilitating 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 todays and tomorrow's digital world, to survive and thrive online.
- Helping 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.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

**1.3 Scope**

This policy applies to all members of the Tetherdown school community (including teaching, supply and support staff, 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.

**1.4 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.

Depending on their role, all members of the school community should read the relevant section below. Please note there is one for All Staff which must be read even by those who have a named role in another section. There are also pupil, governor, etc role descriptions. All staff have a key role to play in feeding back on potential issues.

| Role | Key Responsibilities |
|---|---|
| **Headteacher** | • Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.<br>• 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)<br>• Undertake training in offline and online safeguarding, in accordance with statutory guidance and Local Safeguarding Children Partnership support and guidance.<br>• 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.<br>• 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<br>• 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.<br>• Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the 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.<br>• 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.<br>• 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.<br>• Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.<br>• Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised.<br>• Ensure the school website meets statutory requirements |
| **Designated Safeguarding Lead** | • The DSL should take **lead responsibility** for safeguarding and child protection (**including online safety and understanding the filtering and monitoring** systems and processes in place).<br>• Ensure an effective whole school approach to online safety as per KCSIE.<br>• Ensure the school is complying with the DfE's standards on Filtering and Monitoring.<br>• As part of this, the DSL will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode and preferred search engine/s etc.<br>• Where online safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible, but which cover areas of online safety (e.g. RSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused.<br>• Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online safety) at induction and that this is regularly updated.<br>  ○ This must include filtering and monitoring and help them to understand their roles.<br>  ○ All staff must read KCSIE Part 1 and all those working with children also Annex B – translations are available in 13 community languages at kcsietranslate.lgfl.net (the condensed Annex A can be provided instead to staff who do not directly work with children if this is better)<br>  ○ Cascade knowledge of risks and opportunities throughout the organisation.<br>• Ensure that ALL governors undergo safeguarding and child protection training (including online safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated |

| | |
|---|---|
| | • Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.<br>• Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.<br>• 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.<br>• Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).<br>• Work with the headteacher, DPO 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.<br>• Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.<br>• 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.<br>• Receive regular updates about online safety issues and legislation, be aware of local and school trends.<br>• 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.<br>• Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, including hard-to-reach parents<br>• Communicate regularly with SLT and the safeguarding 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.<br>• 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.<br>• 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. Virtual wellbeing check-ins will be arranged for pupils when off site.<br>• Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).<br>• 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 (acceptable use policy) and those hired by parents. |
| **Governing Body, led by Safeguarding Link Governor** | • 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 .<br>• Undergo (and signpost all other governors 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.<br>• Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.<br>• Safeguarding Governor to work closely with DSL on filtering and monitoring standards standards. Add to Safeguarding governor role<br>• Support the school in encouraging parents and the wider community to become engaged in online safety activities.<br>• Have regular strategic reviews with the online safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.<br>• 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.<br>• Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.<br>• Ensure that all staff undergo safeguarding and child protection training (including online safety and now also reminders about filtering and monitoring.<br>• Ensure that children are taught about safeguarding and online safety, in computing and PHSE lessons. Follow the policy that personal mobile phones are not used at school. |
| **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 staff handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.<br>• Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up<br>• They must report 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 2024) and guidance (such as KCSIE).<br>• Staff should also be aware of the DfE standards for filtering and monitoring and play their part in feeding back to the DSL about |

| | |
|---|---|
| | overblocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.<br>• Know who the Designated Safeguarding Lead (DSL)<br>• Notify the DSL if policy does not reflect practice in the school and follow escalation procedures if concerns are not promptly acted upon<br>• Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)<br>• Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)<br>• Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies<br>• When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.<br>• Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR.<br>• Always be aware of security best-practice, including password hygiene and phishing strategies.<br>• Prepare and check all online source and resources before using<br>• Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.<br>• Notify the DSL/OSL of new trends and issues before they become a problem<br>• Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this)<br>• Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know<br>• Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues<br>• Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff |

| | |
|---|---|
| **PSHE Personal,Social Health and Economics Education Lead and RSHE Relationships, Sex, Health Education Lead** | • As listed in the 'all staff' section, plus:<br>• Embed consent, mental wellbeing, healthy relationships and staying safe online as well as raising awareness of the risks and challenges from latest 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<br>• 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.<br>• 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,.<br>• Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE / RSHE.<br>• Note that an RSHE policy should be included on the school website.<br>• 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** | • As listed in the 'all staff' section, plus:<br>• Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.<br>• Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach.<br>• Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.<br>• 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** | • As listed in the 'all staff' section, plus:<br>• Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.<br>• 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.<br>• Ensure subject specific action plans also have an online safety element. |
| **Network Manager/other technical support roles –** | • As listed in the 'all staff' section, plus:<br>• Collaborate regularly with the DSL and leadership team to help them make key strategic decisions around the safeguarding elements of technology.<br>• Support safeguarding teams to understand and manage filtering and monitoring systems and carry out regular reviews and annual checks .<br>• Support DSLs and SLT to carry out an annual online safety audit as 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 DfE standards, protections for pupils in the home and remote-learning.<br>• 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.<br>• Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact / RSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.<br>• 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.<br>• Ensure filtering and monitoring systems work on new devices and services before releasing them to students and staff.<br>• Maintain up-to-date documentation of the school's online security and technical procedures.<br>• To report online safety related issues that come to their attention in line with school policy.<br>• 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.<br>• Ensure the data protection policy and cyber security policy are up to date, easy to follow and practicable<br>• 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 requirement |
| **Data Protection Officer (DPO)** | • Alongside those of other staff, provide data protection expertise and training and support the DP and cyber security policy and compliance with those and legislation and ensure that the policies conform with each other and with this policy.<br>• 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, "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."<br>• Tetherdown safeguarding records retention until a pupil is 25 years old.<br>• Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited. |
| **Pupils** | • Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually. (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils)<br>• Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors<br>• Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor<br>• Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.<br>• To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media<br>• Treat remote learning in the same way as regular learning in school and behave as if a teacher or parent were watching the screen<br>• Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.<br>• Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems |

| | |
|---|---|
| **Parents/Carers** | • Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it<br>• Consult with the school if they have any concerns about their children's and others' use of technology<br>• 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.<br>• Encourage children to engage fully in home-learning during any period of remote learning and flag any concerns<br>• Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.<br>• If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately. Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online |
| **Volunteers and contractors (including tutor)** | • Read, understand, sign and adhere to an Acceptable Use Policy (AUP)<br>• Report any concerns, no matter how small, to the designated safety lead.<br>• Maintain an awareness of current online safety issues and guidance.<br>• Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.<br>• 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. |
| **Wider school Community - External groups including parent associations, club leaders** | • Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school<br>• Support the school in promoting online safety and data protection<br>• 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<br>• Take responsibility for the security of data.<br>• Develop an awareness of online safety issues, and how they relate to pupils in their care.<br>• Know when and how to escalate online safety issues. |

| | |
|---|---|
| | • Maintain a professional level of conduct in their personal use of technology, both within and outside school.<br>• Take responsibility for their professional development in this area. |
| **Business Manager** | • To ensure that all data held on pupils on the school office machines have appropriate access controls in place |

**1.5 Communication:**

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
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff and those starting mid-year)
- Integral to safeguarding updates and training for all staff
- This policy forms part of the annual INSET (Housekeeping/Health and Safety/Safeguarding)
- 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), which will be issued to whole school community, on entry to the school, annually and whenever changed, plus displayed in school
- Discussed in parent webinars/workshops
- Updates and training for staff in line with new guidance/legislation/policy/concerns.

**1.6 Review and Monitoring**

This policy is a living document, subject to full bi-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 is possible to follow in all respects. This will help all stakeholders to understand the rules that are in place and why. Acceptable Use Policies (see appendix) for different staff, governors, pupils and parents help with this.

**1.7 Current Online Safeguarding Trends**

In our school over the past couple of years, 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:

- **Cyberbullying and Online Harassment:** Reports of cyberbullying incidents through platforms such as WhatsApp and Roblox, with students often using private group chats to exclude or target others. This has had a notable impact on students' emotional wellbeing.
- **Inappropriate Content Exposure**: There have been several incidents of students accessing inappropriate or non-age appropriate content online at home, either intentionally or accidentally. This includes age-inappropriate games, violent videos and explicit material.

These observations have been gathered from a combination of teacher reports, parental feedback and discussions with children.

Nationally, some of the latest trends of the past twelve months are outlined below. These are 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.

Self-generative artificial intelligence has become rapidly more accessible, with many students often having 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 (gen AI can be responsible for incorrect and sometime harmful 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. Self-generative AI has also made it easier than ever to create sexualised images and deepfake videos. Whilst they may not be real, they have a devastating effect on a young person's emotional wellbeing and physical safety, and can also be used to blackmail, humiliate and abuse. The Internet Watch Foundation has reported AI-generated imagery of child sexual abuse progressing at such a worrying rate.

Ofcom's 'Children and parents: media use and attitudes report 2024' 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 (especially with the minimum age for use of WhatsApp now 13). With children aged 3 - 17 spending an average 3 hours 5 minutes per day online, four in ten parents report finding it hard to control their child's screentime. Notably, 45% of 8-11s feel that their parents' screentime is too high, underlining the importance of modelling good behaviour.

Given the 13+ minimum age requirement on most social media platforms, it is notable that half (51%) of children under 13 use them. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third (36%) of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

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 will remind about best practice while remembering the reality for most of our students is quite different.

This is striking when you consider that 25% 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 remains the fastest growing for this form of child sexual abuse material.

Growing numbers of children and young people are using social media and apps such as Snapchat as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news. The alarming speed and scale at which misinformation about the attack in Southport (August 2024) was shared, resulting in Islamophobic and racist violence, rioting and looting across England is particularly concerning, with much of it was fuelled by false online accusations about the assailant. Despite attempts by Police and national news to correct the misleading information, it racked up millions of views on social media sites like X and was actively promoted by several high-profile users with large followings.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm.

Cyber Security is an essential component in safeguarding children and now features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2024 highlighting an increase in school attacks nationally, with 71% of secondary schools reporting a breach or attack in the past year, and 52% of primary schools.
We recommend that parents join the smartfreephonechildhood scheme: Smartphone Free Childhood

# 2.EDUCATION AND CURRICULUM

As a school, we have established a carefully sequenced curriculum for online safety that develops competencies (as well as knowledge about risks) and 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, at Tetherdown we embed teaching about online safety and harms through a whole school approach (assembly, workshops, computing, PSHE, RSHE, newsletter) and provide an understanding of these risks to help tailor teaching and support to the specific needs of pupils, including vulnerable pupils.

At Tetherdown, we recognise that online safety and broader digital resilience must be threaded throughout the curriculum and that is why we have adopted the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). Annual reviews of our curriculum plans / schemes of work (including for SEND pupils) 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
- Copyright and ownership

**Pupil Online Safety Curriculum**

Tetherdown has a clear, progressive Online safety curriculum as part of the Computing / PSHE/ RSHE/ SMSC curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy.
- To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be.
- To know how to narrow down or refine a search.
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings.
- To understand acceptable behaviour when using an online environment / email, i.e. Be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private.
- To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments.
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned on privacy settings.
- To understand why they must not post pictures or videos of others without their permission.
- To know not to download any files – such as music files - without permission.
- To have strategies for dealing with receipt of inappropriate materials.

- [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons.
- To understand the impact of online bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of online bullying.
- To know how to report any abuse including online bullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e., parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button
- To know practical use as well as the ethical pros and cons or using generative AI
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Despite the risks associated with being online, Tetherdown school recognises the opportunities and benefits of children being online. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion.

However, as stated previously, 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.

Whenever overseeing the use of technology (devices, the internet, generative AI tools, etc.) in school or setting as homework tasks, all staff should remind/encourage sensible use, monitor what pupils/students are doing and consider potential risks and the age appropriateness of tasks. This includes supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation and fake news), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.

We communicate with parents and carers about how we support pupils with their online safety learning, including what their children are being asked to do online and the sites they will be asked to access by [e.g. sharing policies, sharing the curriculum, in newsletters, etc.]

**Parent Awareness and Training**

Tetherdown runs a rolling programme of advice, guidance and training for parents, including:

- Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of online safe behaviour are made clear
- Information leaflets; in school newsletters; on the school website.
- Annual Online workshops
- Suggestions for safe Internet use at home.
- Provision of information about national support sites for parents.

# 3. HANDLING ONLINE-SAFETY CONCERNS AND INCIDENTS

It is vital that all staff recognise that online safety is a part of safeguarding and so 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 speak to the safeguarding lead with any concerns (no matter how small these seem) 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.

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

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies (see appendix)
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)
- Cyber Security to be developed –

This school commits to take all reasonable precautions to safeguard 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 and the wider community 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. The reporting member of staff will ensure that a record is made of the concern on EDUKEY - this includes any concerns raised by the filtering and monitoring systems (see section further on in this policy for more information).

Any concern/allegation about staff misuse is always (similar to any safeguarding concern) 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.

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 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 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 (procedures are in place for sexting and upskirting; see section below)

The following sub-sections provide detail on managing types of concern.
Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Governors and the LA.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include

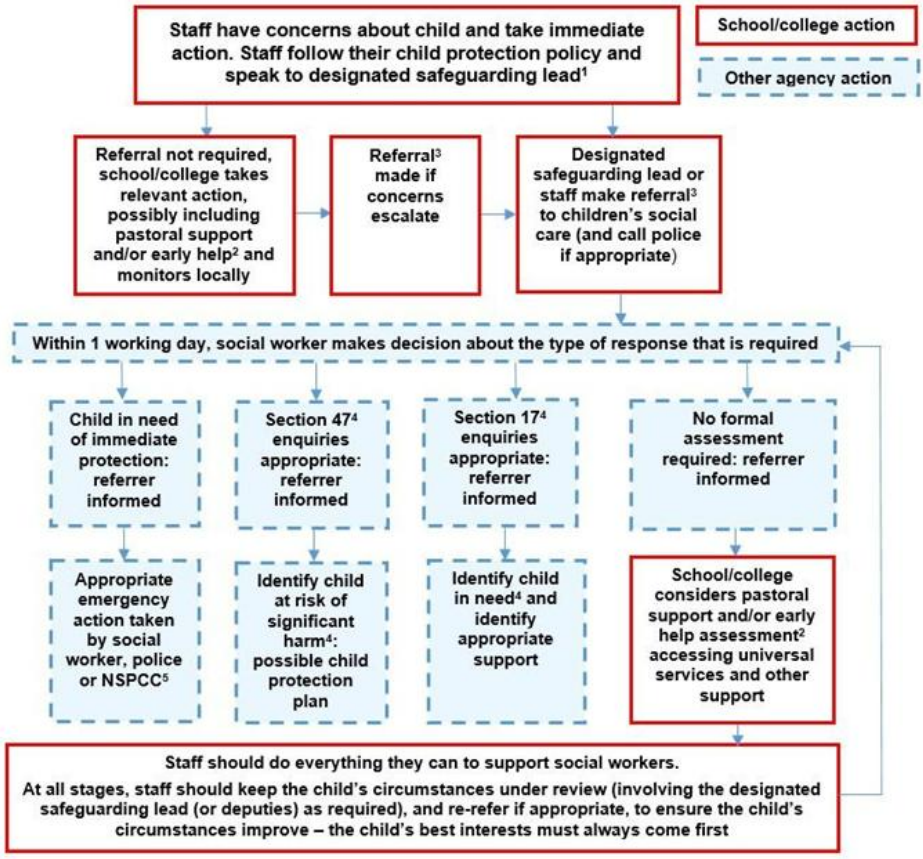
- .Investigations by either teachers, phase leaders or SLT
- Informing parents or carers
- Internal exclusion
- Removal of Internet or computer access
- Referral to LA / Police.

Our DSL acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

**Actions Where There Are Concerns About a Child**

This Actions where there are Concerns about a Child Flow Chart is taken from (page 24) KSCSIE September 2024. Online safety concerns are no different to any other safeguarding concern.




**Sexting - Nudes – sharing nudes and semi-nudes**

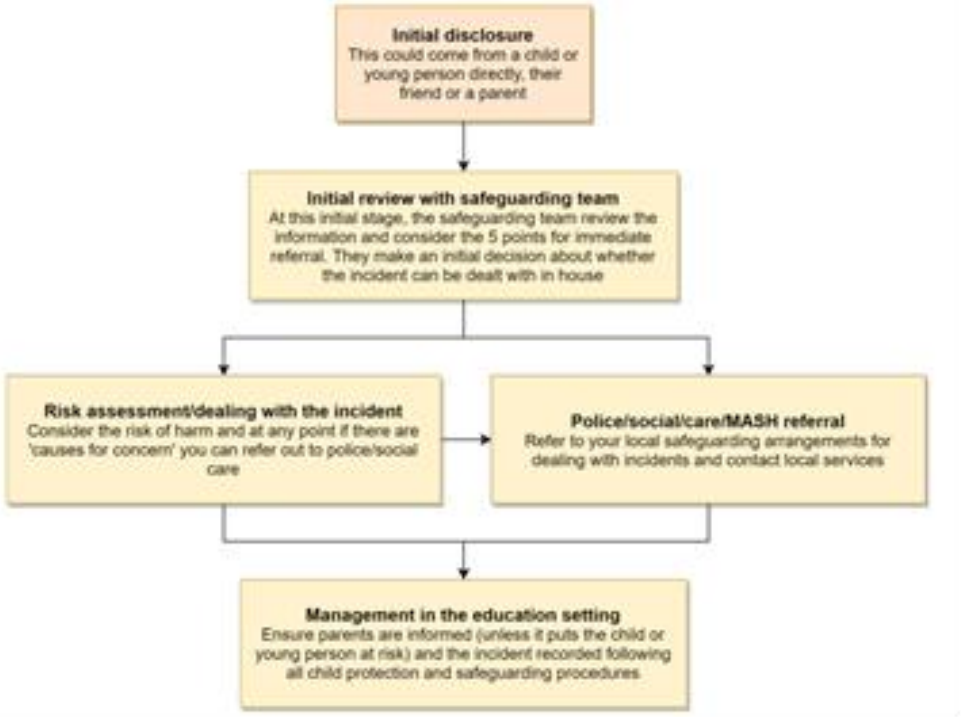
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings.

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based 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**.

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, students should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will 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 (see flow chart below from the UKCIS guidance) and next steps regarding liaising with parents and supporting pupils.

.




## Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse 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 (which may also be referred to as cyberbullying), including incidents that take place outside of school should be treated like any other form of bullying and the school bullying policy should be followed, this includes issues arising from banter.

**Child-on-child sexual violence and sexual harassment**

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in KCSIE. 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. This will be discussed in staff training.

**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 (see appendix) 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 handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

**Social Media Incidents**

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the safeguarding policy. Other policies that govern these types of incidents are the school's Acceptable Use Policies (see appendix).

Breaches will be dealt with in line with the school behaviour policy (for pupils) or staff handbook. See the social media section later in this document for rules and expectations of behaviour for children and adults in the Tetherdown school community. Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community (e.g. parent or visitor), we will request that the post be deleted and will expect this to be actioned promptly.

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

**Extremism**

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

**Use of Generative AI**

At Tetherdown, we acknowledge that generative AI platforms (e.g. ChatGPT or Bard for text creation or the use of Co-Pilot or Adobe Firefly to create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on this. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons. This is communicated through online safety and computing lessons, staff insets and online safety parent workshops.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some students – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).

# 4.MANAGING THE IT AND COMPUTING INFRASTRUCTURE

**Network management (user access, backup)**

*This school*

- Uses individual, audited logins for all users - the London USO system and Microsoft teams. We recommend that staff change their passwords on any secure system, every 90 days / twice a year.
- Uses guest accounts occasionally for external or short-term visitors for temporary access to appropriate services
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful.
- Has additional local network auditing software installed.
- Ensures the Systems Administrator / network manager is up to date with LGfL services and policies / requires the Technical Support Provider to be up to date with LGfL services and policies.
- Storage of all data within the school will conform to the UK data protection requirements
- All pupils have their own unique username and password
- Requires all users to always log off when they have finished working or are leaving the computer unattended. Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Maintains equipment to ensure Health and Safety is followed.
    - e.g., projector filters cleaned by site manager / TA; equipment installed and checked by approved Suppliers / LA electrical engineers
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.
    - e.g., teachers access report writing module; SEN coordinator - SEN data.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.
    - e.g., technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child.

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data, which complies with external Audit's requirements.
- All computer equipment is installed professionally and meets health and safety standards.
- Reviews the school IT systems regularly with regard to health and safety and security.

**Data Protection and Data Security**

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection and cyber security policy. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children.

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 2024, "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**

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.

The designated safeguarding lead (DSL) has lead responsibility for filtering and monitoring and works closely with TurnItOn to implement the DfE filtering and monitoring standards, which require schools 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.

We look to provide 'appropriate filtering and monitoring (as outlined in Keeping Children Safe in Education) at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems 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 TurnItOn and will be asked for feedback at the time of the regular checks which will now take place. We carry out half-termly checks to ensure all systems are in operation, functioning as expected, etc and an annual review as part of an online safety audit of strategy, approach etc. These are also used to ensure that the school responds to any issues and integrates with the curriculum.

Safe Search is enforced on any accessible search engines on all devices.
We recommend the use of Kiddle - visual search engine for kids.

Our YouTube mode is on moderate restricted.

Out of hours, our policies are:

- Filtering reports are run during evenings, weekends and holidays but are not looked at during holidays.
- Monitoring alerts are not looked at during evenings, weekends or holidays but will be picked up in office hours.

The DSL checks filtering reports and notifications monthly and takes any necessary action as a result.

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 (Microsoft 365 Admin console for Windows devices and Meraki for iPads)
- network monitoring using log files of internet traffic and web access (LGFL services, DHCP services and Microsoft admin console)
- individual device monitoring through software or third-party services

For staff:

- What is monitored? emails, browsing history, device usage.
- When monitoring applies? only on school devices or networks, or personal devices if they are using school network.
- Who has access to reports and under what circumstances? DSL

*This school*:

- Has the educational filtered secure broadband connectivity through LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- Ensures network healthy through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files.
- Uses DfE, LA or LGfL approved systems such as S2S, USO FX, secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network
- Uses security time-outs on Internet access where practicable / useful.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's learning platform as a key way to direct students to age / subject appropriate web sites; plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g., google safe search
- Informs all users that internet use is monitored

Informs staff and students that that they must report any failure of the filtering systems directly to the IT system adminstrator. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGFL helpdesk as necessary.

**CCTV**

Our CCTV storage and usage align with GDPR/Data Protection Act and ICO guidance on CCTV use.

- Retention period: Footage is stored for 3 months.
- Secure storage: Footage is stored in an encrypted and access-controlled system.
- Accessed only by authorized personnel.

## 5. ELECTRONIC COMMUNICATIONS

**Authorised systems**

Staff at this school use the email system provided by Microsoft 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 school staff, parents and external organisations.

Staff at this school use ParentPay/Arbor to communicate with Parents when concerning the school and child data.

Any systems above are centrally managed and administered by the school or authorised TurnItOn (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. 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.

**School Website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website and ensuring compliance with DfE stipulations. The website is managed by our Communications Officer.

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.

**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 photography/images, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For use within school premises (e.g.displays around the school)
- For use on the school website (e.g. newsletter)
- For use in print media (e.g. paper-based school marketing)
- For use internet/online media including social networks, apps or websites
- For use by school photographer (made available for parents to purchase)
- For use in broadcasting media

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 Tetherdown, 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 Teams secure storage  secure storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

Staff and parents are reminded annually about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection (e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. 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 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.

**Cloud 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 cyber security before always adopting such a platform or service and when using it.

## Social Media

Tetherdown 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.

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. Tetherdown is responsible for managing our Instagram social media account and checking our Wikipedia and Google reviews and other mentions online.

## Staff, pupils' and parents' Social Media 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 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 but the school regularly deals 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 and not encourage or condone underage use. However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/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 (parents don't need to know them to ask their child to explain it to them), 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). Parents 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 Instagram 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.

As outlined in the Acceptable Use Policies, pupils/students 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 considerable 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 this school policy link to social media management for staff (in Staff Handbook and Social Media in school policy) and to seek permission before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

## 6. DEVICE USAGE

**Personal Devices Including Wearable Technology**

- **Student mobile phones are strongly discouraged.** Independent travellers in Y5 and 6 are allowed to bring mobile phones in for emergency use only**.** Phones must remain turned off on the school premises and handed into the class teacher in the morning. 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. Parents/Carers are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during break times. 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 on in the class. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off or on silent. Under no circumstances should they be used in the presence of children/staff or to take photographs, voice recordings 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 and turned off/ silent when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children or of voice recordings of meetings. Please see the Digital images and video section of this document for more information about filming and photography at school events and please refer to Parents Use of Social Media Policy on our website policy pages.
- Where BYOD is allowed, neither staff nor students are allowed to use a mobile hotspot to provide internet to the device as this would potentially bypass filtering in contravention of AUPs.
- The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.

**Use of school devices**

- School owned, staff-handheld devices, including school mobile phones and school cameras must be noted in school – name, make & model, serial number. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff and pupils are expected to follow the terms of the school acceptable use policies for appropriate use and behaviour when on school devices, whether on site or at home. School devices are not to be used in any way which contravenes AUPs, behaviour policy / staff code of conduct.
- Wi-Fi is accessible to Staff for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- Volunteers, contractors, governors have can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- School devices for staff or students are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable as well as appropriate personal use.

**Trips / events away from school**

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with parents. Teachers using their personal phone will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number

Whilst Parents are on trips not take photographs to share on social media without permission – See Parents Social Media Policy .

On trips (especially residential) children are not encouraged to bring any mobile phones or smart watches.

**Searching and confiscation**

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example because of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

Full details of the school's search procedures are available in the school Behaviour Policy. DFE guidance : https://www.gov.uk/government/publications/searching-screening-and-confiscation

**Asset Tracking and disposal**

Details of all school-owned hardware will be recorded in a hardware inventory. Details of all school-owned software will be recorded in a software inventory. All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

## APPENDICES:

1. Acceptable Use Agreement (Staff/Governors/Volunteers)
2. Acceptable Use Agreement (KS2 Pupils)
3. Acceptable Use Agreement (KS1 Pupils)
4. Acceptable Use Agreement including photo/video permission (Parents)
5. Protocol for responding to Online safety incidents

# *1.* Acceptable Use Agreement for Staff, Governors and Volunteers

We ask everyone involved in the life of Tetherdown to sign an Acceptable Use Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

1. **(This point is for staff and governors):**
   I have read and understood Tetherdown's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our online safety policy which describes trends over the past year at a national level and in this school.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I identify.
4. I will follow the guidance in the Safeguarding and Online Safety policies for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media)
5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture; online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take a zero-tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying and sexual violence & harassment – knowing that 'it could happen here'!
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).
9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk with pupils about appropriate behaviour and

how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).

10. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
11. I will prepare and check all online sources and classroom resources **before** using them, for accuracy and appropriateness. I will flag any concerns about "overblocking" to the DSL.
12. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
13. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
14. During any periods of remote learning, I will not behave any differently towards students compared to when I am in school and will follow the same safeguarding principles as outlined in the main child protection and safeguarding policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
15. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, can be monitored/captured/viewed by the relevant authorised staff members.
16. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils or adults may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.
17. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
18. I will not contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the headteacher.
19. I will not use a mobile hotspot to provide internet to any device I use in school.
20. I agree to adhere to all provisions of the school's Cybersecurity and Data Protection Policies Section 8 of the school's Data Protection Policies at all times, whether I am on site or using a school device, platform or network.
21. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an

education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

22. I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature. I understand that any breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.
23. I will only use generative AI platforms that have been authorised for use, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.

---

***To be completed by Governors/Staff/Volunteers***

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

**Signature:** _____

**Name:** _____

**Role:** _____

**Date:** _____

Laptop: Model
Make
Security Tag
Haringey Security Tag

iPad: Security Tag
Haringey Security Tag

## 2. Key Stage 2 Pupils Acceptable Use Online Safety agreement

**For my own personal safety – everywhere!**

I will ask permission from a member of staff before using the Internet at school.

I am aware of “stranger danger” when online and will not agree to meet online friends.

I will tell an adult about anything online which makes me feel uncomfortable.

I will not try to bypass the system to reach websites the school has blocked.

I understand that the school may check my files and may monitor the web pages I visit.

When in school I will only contact people with my teacher’s permission.

I know it's not my fault if I see or someone sends me something bad - I don't need to worry about getting in trouble, but I mustn't share it. Instead, I will tell a trusted adult.

**To keep the system safe**

I will only use my own login and password, which I will keep secret.

I will not access other people's files.

I will not play games on a school computer unless my teacher has given me permission.

I will not install software on school computers.

I will not use the system for gaming, gambling, shopping, or uploading videos or music.

I will be very careful when sharing pictures or video of myself or my friends.

If I am in school, I will always check with a teacher.

I will not put my “Personal Information” online. (My full name, birthday, phone number, address, postcode, school etc.)

I keep my body to myself online – I never get changed or show what’s under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don’t send any photos or videos without checking with a trusted adult.

I follow age rules – 13+ games, apps and films aren’t good for me so I don’t use them – they may be scary, violent or unsuitable. 18+ games are very unsuitable.

**Responsibility to others**

The messages I send will be polite and responsible.  I will be kind.

I will not upload images or video of other people without their permission.

Where work is copyrighted (including music, videos and images,) I will not download or share with others. I will always quote the source of any information gained from the Internet, i.e., the web address, in the documents I produce.

I understand that if I do something unkind or unsafe online or on a device, or if I see it and don't tell an adult, the school will use the behaviour policy to decide what happens, depending on how serious it is.I will avoid any acts of vandalism. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.

I understand that if I don't follow these rules, my access to the school computer, iPad, network system/Internet/Email may be suspended, and my parents/carers will be informed

**Personal Devices**

It is not permitted for pupils to use smart Phones or smart watches linked to mobile data during the school day. An exception may be made.for those children who may use them for medical reasons

Teachers can search my property on school premises. This includes the content of mobile phones and other devices.

Other devices (e.g., Games consoles, cameras, Apple watches or similar) should not be brought into school, unless my teacher has given me permission. The school cannot accept responsibility for loss or damage to personal devices.

**Pupil name: _____ Class_____**

☐ **I have read the school 'rules for online safety'. My teacher has explained them to me.**

☐ **I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.**

☐ **This means I will use the computers, iPad, Internet, e-mail, online communities, digital cameras, video recorders and other computing devices in a safe and responsible way.**

☐ **I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, that they may contact my parent / carer.**

**Pupil's signature _____Date: _____/_____/_____**

*Teachers: Once signed by the pupil, please send a signed copy home for parents.*

# 3. Key Stage 1 Pupils Acceptable Use Online Safety agreement

TICK

I **KNOW** who my trusted adults are

I only **USE** devices or apps, sites or games if I am allowed to.

I will **CHECK** with a trusted adult before I use any website, game on app

I **ASK** for help if I'm stuck or not sure; I will **TELL** a trusted adult if I get upset, worried, scared or confused when I am online

If I get a **FUNNY FEELING** in my tummy, I talk to an adult

I **KNOW** that online people aren't always who they say they are and things I read or see are not always **TRUE**.

I am **KIND** and polite to everyone

I will **NOT SHARE** my password

I **STAY SAFE** because I never share private things like my name address or telephone number

Anything I do online can be shared and might stay online FOREVER

I will **NOT KEEP SECRETS** or do **DARES and CHALLENGES** just because someone asked me to

I don't change **CLOTHES** in front of a camera

**STRANGER DANGER** - I know that people online aren't always who they say they are

My trusted adults are:
_____ at school
_____ at home

**Pupil name: _____**

**Class_____ Date: ___/_____/_____**

# 4. Acceptable Use Agreement including photo/video permission (Parents)

*These permissions are shared with Parents through Admissions.*

**Online Safety**

As part of the school's Computing curriculum, we offer pupils supervised access to an educationally filtered internet service. and restricted access e-mail. Further details of our online safety policy is available on our website.

I understand that my child (Y1-6) will also sign an online safety agreement form and that their teacher will discuss responsible use (introduced over several online safety lessons).

I confirm I have read the statement

> *I give permission for my child to have access to and use the Internet, blogging, e-mail and other ICT facilities at school.*
> *I understand that my child in Middle and Upper Phase (Y2-6) will also sign an online safety agreement form and that their teacher will discuss responsible ICT use (introduced over several online safety lessons).*

**Use of digital images, photography and video**

> I understand the school has a clear policy on 'the use of digital images and video' and I support this.
> I understand that the school will necessarily use photographs/images of my child or include them in video material to support learning activities.

I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities. There is a section below where you will be able to provide your specific consent in relation to the use of images of your child. This statement is confirming that you have understood the school has an online safety policy in place and the policy is available on our website

**Social networking and media sites**

1. I understand that the school has a clear policy on 'The use of social networking and media sites' and I support this.
2. I understand that children are not allowed to bring mobile phones into school. If children are independent travellers (Y5/6) they may bring mobile phones which will be kept with the teacher throughout the day. rewrite for Y5/6
3. I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.
4. I will support the school by promoting safe use of the internet and digital technology at home and I will inform the school if I have any concerns. I understand that I will not take and then share online, photographs , videos or voice recordings of other children (or staff) at school events without asking permission from the children's parents or staff

5. This statement is confirming that you have understood the school has an online safety policy in place and the policy is available on our website

**Photography / Images Consent**

As you may be aware, the General Data Protection Regulation came into force on the 25th May 2018. This has placed additional obligations on organisations and affects how they handle data. We take cyber security and data protection very seriously and we have put steps in place within our organisation to ensure we maintain secure and compliant systems.

As a school, we regularly use photographs to show how our pupils and the school develop. Images can also help us illustrate and communicate with parents about upcoming events and can help advertise and market the school to prospective parents and pupils. We are also aware that parents and pupils really enjoy being able to see their images and would like to give all pupils this opportunity.

There are several instances when the school may take photos of your child, specifically: -

- We publish photos on the school's website to promote the school to current and prospective parents as well as providing updates on current events;
- We publish photos on our social media account Instagram to provide updates on events and news within the school;
- Within our Newsletters, we may provide photos of recent events or achievements from our pupils;
- In order to promote the school, we send out prospectuses, flyers, leaflets and brochures which contain images to show life at our school. These will be sent to prospective parents;
- We may also use other promotional materials such as banners and signs which may contain photographic images for prospective parents to view;
- We may be visited by the media who may take photographs or film footage of events. Pupils will sometimes appear in these images, which may then be published in local or national newspapers, in televised news programmes and on social media sites;
- We publish photos in and around the school building to illustrate to current pupils and parents life around our school, including educational materials and images of recent trips and events. These can be seen from time to time by other parents or visitors within the school;
- In promotional materials to show the history and character of the school to future generations.
- Up to twice a year a school photographer will visit the school and take individual and group photos of the children which will be made available to purchase. Reminders will be sent in good time prior to the visit.

We follow guidance as set by data protection legislation (mainly the General Data Protection Regulation) as well as guidance set by the Information Commissioner's Office on taking photos in schools and obtaining consent. The school will consider preferences set out below.

• Usually, pupils will not be named in the photographs unless they gain specific consent in the first instance.
• Consent to using your child's images will last throughout your child's time at the school and will continue to apply for a short time after they leave (except for images published for historical purposes which may be kept for an extended period to show the history of the school). Your child is likely to be photographed or filmed while engaging in the curriculum at Tetherdown.

The school will not seek to reaffirm photography/images consents provided but will on a case-by-case basis communicate with parents in advance for selected events.

Once images are published externally, for example, on social media and on the school website, the images are no longer within the school's control and copies may be taken and published elsewhere by third parties.

We would like to seek your consent for the use of your child's images and will respect your decisions when publishing photos moving forward. You can withdraw your consent at any time and can do so by emailing our Business Manager, at businessmanager@tetherdownschool.org asking the school to stop using your child's images. At that point they will not be used in future publications, but we cannot prevent them from continuing to appear in publications already in circulation. For further information on what we collect, hold and share, and the reasons why please refer to our Privacy Notice for Pupils and Parents available on our website policy page. **Please indicate below whether you grant or deny permission by ticking the box next to the consent request.**

Use of photograph by school photographer (made available for parents to purchase)

Use of photography/images for internet/online media including social networks, apps or websites (e.g. Facebook, Instagram, X)

Use of photography/images in broadcasting media distribution of content, either audio or video (e.g. radio, TV). We may be visited by the media who will take photographs or film footage of events. Pupils will sometimes appear in these images, which may then be published in local or national newspapers, in televised news programmes and on social media sites.

Use of photography/images in print media including but not limited to publications, brochures, banners, prospectuses, leaflets, displays, newspapers, magazines and books.

Use of photography/images on school website

Use of photography/images within school premises. These can be seen occasionally by other parents or visitors within school.

## 5. Guidance: What do we do if?

**An inappropriate website is accessed unintentionally in school by a teacher or child.**

1. Play the situation down; don't make it into a drama.
2. Report to the head teacher online safety officer and decide whether to inform parents of any children who viewed the site.
3. Inform the school technicians and ensure the site is filtered (LGfL schools report to: Atomwide via the LGFL Helpdesk).
4. Inform the LA if the filtering service is provided via an LA/RBC.

**An inappropriate website is accessed intentionally by a child.**

1. Refer to the acceptable use policy that was signed by the child and apply agreed sanctions.
2. Notify the parents of the child.
3. Inform the school technicians and ensure the site is filtered if need be.
4. Inform the LA if the filtering service is provided via an LA/RBC.

**An inappropriate website is accessed intentionally by a staff member.**

1. Ensure all evidence is stored and logged
2. Refer to the acceptable use and staffing policy that was signed by the staff member and apply disciplinary procedure.
3. Notify governing body.
4. Inform the school technicians and ensure the site is filtered if need be.
5. Inform the LA if the filtering service is provided via an LA/RBC.
6. In an extreme case where the material is of an illegal nature: Contact the local police and follow their advice.

**An adult uses School IT equipment inappropriately.**

1. Ensure you have a colleague with you, do not view the misuse alone.
2. Report the misuse immediately to the head teacher (or named proxy) and ensure that there is no further access to the device. Record all actions taken.
   - If the material is offensive but not illegal, the head teacher should then: Remove the device to a secure place.
   - Instigate an audit of all ICT equipment by the schools ICT managed service providers or technical teams to ensure there is no risk of pupils accessing inappropriate materials in the school.
   - Identify the precise details of the material.
   - Take appropriate disciplinary action (undertaken by Headteacher). Inform governors of the incident.
3. In an extreme case where the material is of an illegal nature: Contact the local police and follow their advice. If requested to remove the device to a secure place and document what you have done.

All of the above incidences must be reported immediately to the head teacher and online safety officer.

**A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of school time.**

1. Advise the child not to respond to the message.

2. Refer to relevant policies including online safety anti-bullying and PHSE and apply appropriate sanctions.
3. Secure and preserve any evidence through screenshots and printouts.
4. Inform the sender's e-mail service provider if known.
5. Notify parents of all the children involved.
6. Consider delivering a parent workshop for the school community.
7. Inform the police if necessary.
8. Inform other agencies if required (LA, Child protection, LGFL)

**Malicious or threatening comments are posted on an Internet site (such as social networking) about member of the school community (including pupils and staff).**

1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html.
4. Endeavour to trace the origin and inform police as appropriate.
5. Inform LA and other agencies (child protection, Governing body etc).

The school may wish to consider delivering a parent workshop for the school community

**You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites or gaming) to make inappropriate contact with the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement police and social services.
5. Inform LA and other agencies.
6. Consider delivering a parent workshop for the school community.

**You are concerned that a child's safety is at risk because you suspect they are playing computer games that are inappropriate or certificated beyond the age of the child**

1. Report to and discuss with the named child protection officer in school and contact parents.
2. Advise the child and parents on appropriate games and content. You may want to use LGFL template letters to inform all or targeted parents.
3. If the game is played within school environment, ensure that the technical team block access to the game
4. Consider the involvement social services and child protection agencies.
5. Consider delivering a parent workshop for the school community.

You are aware of social network posts and pages created by parents about the school. While no inaccurate information is posted, it is inflammatory and disruptive, and staff are finding it hard not to respond.

1. Contact the poster or page creator and discuss the issues in person 2. Provide central staff training and discuss as a staff how to behave when finding such posts and appropriate responses.
3. Contact governing body and parent association
4. Consider delivering a parent workshop for the school community.

All the above incidences must be reported immediately to the head teacher and online safety officer.

Children should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.