Policy for

Online Safety

Contents

Governor Responsibility:	Learning & Community Committee
Staff Responsibility:	Reviewed by R Binger
Review Period:	Bi-annual
Status:	Non-statutory
Reviewed:	Spring 2022
Next Review Date:	Spring 2024
Computing Governor:	
Governor Signature	

1. INTRODUCTION AND OVERVIEW

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' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, SMSC and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Aims/Rationale

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich their learning.

The key principles expected of all members of the school community at Tetherdown regarding online behaviour, attitudes and use of digital technology are:

- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates, school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world for:
    - The protection and benefit of the children and young people in their care, and for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.

  - The benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession. Assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

The main areas of risk for our school community can be summarised as follows:

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many new risks are mentioned in KCSIE 2021, e.g., extra-familiar harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future remote learning and lockdowns, there is a greater risk of grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices.

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites
- Radicalisation
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming
- Online bullying in all forms
- Identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (internet or gaming)) sexting (sending and receiving of personally intimate images) also referred to as SGI (self-generated indecent images)
- Extremism
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

Scope

This policy applies to all members of Tetherdown community (including staff, governors, students / pupils, supply teachers, tutors engaged under the DfE National Tutoring Programme, volunteers, contractors, parents / carers, visitors, community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time.

Tetherdown will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online safety behaviour that take place out of school.

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.

Role	Key Responsibilities
Headteacher	• Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguard. • Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding • Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported • Ensure that policies and procedures are followed by all staff • Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships • Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information • Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information • Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles • Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles • Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident

	• Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised • Ensure that there is a system in place to monitor and support staff (e.g., network manager) who carry out internal technical online-safety procedures • Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety • Ensure the school website meets statutory requirements •Ensure that appropriate funding is allocated to support e-safety activities throughout the school (i.e., workshops for children, parents and staff)

Designated Safeguarding Leads **Online Safety Co-ordinator**	• The DSL may delegate certain online safety duties, e.g., to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2021): • “The designated safeguarding lead has lead responsibility for safeguarding and child protection (including online safety).” With the Online Safety Co-ordinator, they should ensure that: • There are regular reviews and open communication between the DSL and OSL, but the DSL has clear overarching responsibility for online safety. • There is “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.” • To “Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs,) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies.” • To “liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children” • To take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns • To 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 • To work with the Headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, whilst ensuring that child protection is always prioritised and data-protection processes support careful and legal sharing of information; 6 Staying up to date with the latest trends in online safety. • To 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 Safeguarding and Child Protection, hole School Behaviour and Anti-bullying, Prevent and others) and submit for regular review to the governors. • To stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training. • 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 • To receive regular updates in online safety issues and legislation, be aware of local and school trends • To promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents/carers, who are often appreciative of school support in this area, but also including hard-to-reach parents. • To liaise with school technical staff, and support staff as appropriate. • Regular communication with SLT and the designated Safeguarding Governor to discuss current issues (anonymised), review incident logs and review filtering and monitoring. • 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. • Adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in

	isolation/quarantine/lockdown, e.g., a safe, simple, online form on the school home page about ‘something that’s worrying me’ that gets mailed securely to the DSL inbox. • appropriate filtering. monitoring and technical support is discussed with governors and staff made aware. • Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying. • Training and advice for all staff is provided to: • Read KCSIE Part 1 and all those working with children Annex A. • Be aware of Annex D (online safety). • And cascade knowledge of risks and opportunities throughout the organisation. • To work with the Headteacher and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards • Particular attention is paid to online tutors, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP- See appendix, and those hired by parents - share the Online Tutors – Keeping Children Safe poster at Home (lgfl.net) to remind parents of key safeguarding principles

Governing Body, led by Safeguarding Link Governor	•Support the Headteacher and/or designated online-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe computing learning environment. •Ensure that appropriate funding is authorised for online safety solutions, training and other activities as recommended by the headteacher and/or Online Safety coordinator (as part of the wider remit of the Governing Body with regards to school budgets). • Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board • Ask about how the school has reviewed protections for pupils in the home (including when with online tutors) and remote-learning procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology. • Support the school in encouraging parents and the wider community to become engaged in online safety activities • Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings • Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised • Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information • Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B; check that Annex D on Online Safety reflects practice in your ￼school • Ensure that all staff undergo safeguarding and child protection training, including online safety at induction. The training should be regularly updated in accordance with the Safeguarding and Child Protection Policy. • Check appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". LGfL's appropriate filtering submission is here • Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school approach to online safety [with] a clear policy on the use of mobile technology." NB – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach
All Staff	• Read, understand, sign and adhere to an acceptable use policy (AUP) • Pay particular attention to safeguarding provisions for home-learning and remote-teaching technologies • (Recognise that RSHE is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject) • Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up

	• Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are • Read Part 1, Annex B and Annex D of Keeping Children Safe in Education • Read and follow this policy in conjunction with the school's main safeguarding policy • Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures using EduKey. • Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself • Sign the Staff Acceptable Use Policy and follow the school's Code of Conduct • Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon • Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils) • Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place) • When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning. • Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and GDPR. • Be aware of security best-practice at all times, including password hygiene and phishing strategies. • Prepare and check all online source and resources before using • Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions. • Notify the DSL/OSL of new trends and issues before they become a problem • Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this) • 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 • Receive regular updates from the DSL/OSL and have a healthy curiosity for online safeguarding issues • Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

PSHE/RSHE Lead	• As listed in the 'all staff' section, plus: • Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age-appropriate way that is relevant to their pupils' lives." • This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies. • Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messages within Spiritual, Moral, Social, Cultural (SMSC)/Religious Education (RE) /RSHE) • Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach
Computing Curriculum Lead/Online Safety	• As listed in the 'all staff' section, plus: • Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum • Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach • Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements • 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
Subject Leads	• As listed in the 'all staff' section, plus: • Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike • Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context • Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing • Ensure subject specific action plans also have an online-safety element
Network Manager/technician (Turn IT On)	• As listed in the 'all staff' section, plus: • Support the HT and DSL team as they review protections for pupils in the home and remote-learning procedures, rules and safeguards • Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa and ensure no conflicts between educational messages and practice.

	• Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy • Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc • Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team • Maintain up-to-date documentation of the school's online security and technical procedures • To report online-safety related issues that come to their attention in line with school policy • Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls • Work with the Headteacher to ensure the school website meets statutory DfE requirements
Data Protection Officer (DPO)	• Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document: • "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children." • The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records. An example of an LA safeguarding record retention policy can be read at safepolicies.lgfl.net, but you should check the rules in your area. • Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. • Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutors)	• Read, understand, sign and adhere to an acceptable use policy (AUP) • Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP • Maintain an awareness of current online safety issues and guidance • Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications • Note that as per AUP agreement a contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
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) • Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen • Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors • Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor • Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else. • To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media • Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher. • Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems
Parents/Carers	• Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it • Consult with the school if they have any concerns about their children's and others' use of technology • Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers. • Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns • Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible. • If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the

	child or attempt to communicate privately. 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
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 • Support the school in promoting online safety and data protection • Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers • Take responsibility for the security of data. • Develop an awareness of online safety issues, and how they relate to pupils in their care. • 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. • 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

Communication:

The policy will be communicated to staff/ pupils/ school community in the following ways:

- Policy to be posted on the school website and network
- Policy to be part of school induction pack for new staff
- This policy forms part of the annual INSET (Housekeeping/Health and Safety/Safeguarding)
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Online safety rules shared with pupils and signed at the beginning of academic year
- Acceptable use agreements to be held in pupil and personnel files
- Updates and training for staff in line with new guidance/legislation/policy/concerns.

Review and Monitoring

The Online safety policy is referenced from within other school policies and documents:

Computing policy, Safeguarding and Child Protection policy, policy, Behaviour and Anti-Bullying policy, Personal, Social and Health Education and RSE policy, GDPR Suite of Policies

- The school has an Online safety coordinator who will be responsible for document ownership, review and updates.
- The Online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The Online safety policy has been written by the school Online safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PSA. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

2.EDUCATION AND CURRICULUM

Pupil Online Safety Curriculum

Tetherdown has a clear, progressive Online safety education programme as part of the Computing / PSHE/ RSHE/ SMSC curriculum. It is built on LA / LGfL online safeguarding and online literacy framework for EYFS to Y6/ national guidance. 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

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

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.

- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying online; online gaming / gambling.

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

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g., fake news), age-appropriate materials and signposting, and legal issues such as copyright and data law.

At Tetherdown, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans / schemes of work (including for 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.

Staff And Governor Training

This school:

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

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.
- Demonstrations, practical sessions held at school.
- Suggestions for safe Internet use at home.
- Provision of information about national support sites for parents.

Expected Conduct

At Tetherdown, ALL USERS:

- Are responsible for using the school Computing systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils.)

- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking / use of images and on online bullying

Staff

- Are responsible for reading the school's Online safety policy and using the school Computing systems accordingly, including the use of mobile phones, and handheld devices.

Students/Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

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

3. HANDLING ONLINE-SAFETY CONCERNS AND INCIDENTS

It is vital that all staff recognise that online safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and SMSC).

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

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
- Sexual Harassment / Peer on Peer Abuse Policy
- Anti-Bullying and Behaviour Policy
- Acceptable Use Policies
- Prevent Policy
- GDPR Suite of Policies, agreements and other documentation (e.g., privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact 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.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

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).

We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in e-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

- Interview/ teachers/Phase-leader / Online Safety Coordinator / Headteacher.
- Informing parents or carers
- Removal of Internet or computer access for a period,

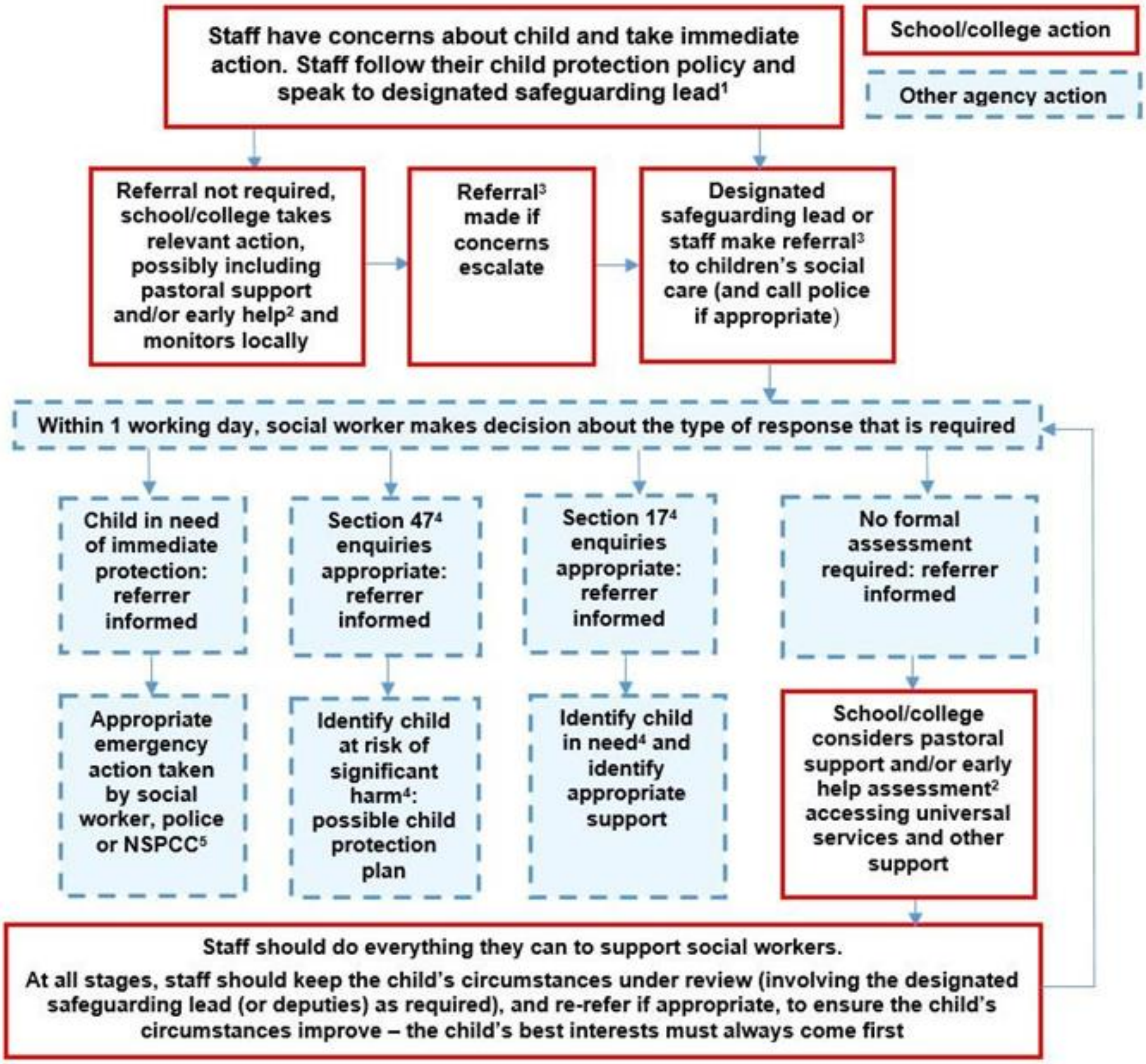
- Referral to LA / Police.

Our Online Safety Coordinator 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 22) KSCSIE September 2021. Online safety concerns are no different to any other safeguarding concern.


Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

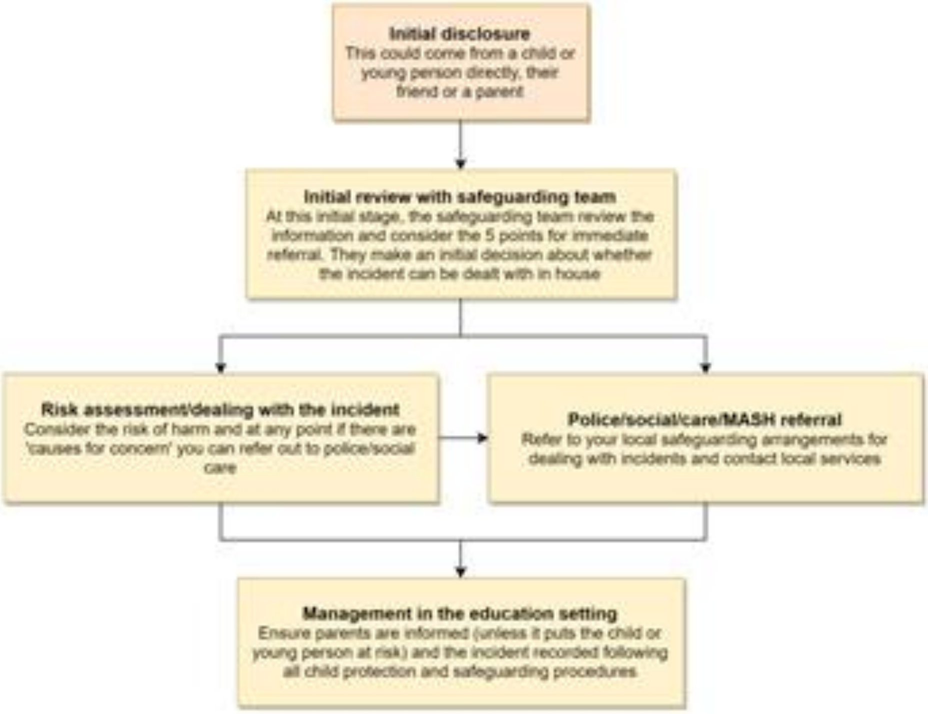
Sexting

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

There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (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.

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



Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures

Consider the 5 points for immediate referral at initial review:

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

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

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

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

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

Sexual Violence and Harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. 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.

Misuse Of School Technology (Devices, Systems, Networks or Platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook.

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

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

Social Media Incidents

Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Tetherdown 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.

School-Safe Video-Sharing Platform

YouTube has many educational videos available for staff to incorporate in lessons but there are many inappropriate videos available online and it is a challenge to filter them and still retain access to those you want to see. The Autoplay function can promote opportunities for tenuously related videos to be played after the original choice. If a video leads into a highly inappropriate one, staff may be associated with it in viewers minds and staff may have no control over linked content or advertising.

Staff must always check videos before using them and use a school-safe platform like LGfL TRUSTnet's Video Central HD (vchd.lgfl.net), which has no adverts, is designed for use with pupils, and is linked to school accounts.

4.MANAGING THE IT AND COMPUTING INFRASTRUCTURE

Data Protection and Data Security

The Department for Education document KCSIE (September 2021 states that the:

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

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

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

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements. The school ensure that all staff sign its Acceptable Use Policy which makes clear all responsibilities and expectations with regard to data security.

The school has approved educational web filtering (see below) across our wired and wireless networks. We can monitor emails, blogs and online platforms to ensure compliance with the Acceptable Use Policy.

Staff have secure areas on the network to store documents and photographs.
The school asks staff to undertake house-keeping checks at least annually to review, remove and destroy any digital materials and documents which no longer need to be stored.

Appropriate Filtering and Monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

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.

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

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

This school:

- Has the educational filtered secure broadband connectivity through the
- LGfL and so connects to the 'private' National Education Network.
- Uses the LGfL Net Sweeper filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status.
- Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students.
- 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
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable / useful.
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Ensures pupils only publish within an appropriately secure environment: the school's learning environment/ the London learning platform/ lgfl secure platforms such as j2bloggy, etc.
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's learning platform as a key way to direct students to age / subject appropriate web sites; plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required; e.g., google safe search , …..
- Never allows / is vigilant when conducting 'raw' image search with pupils e.g., google image search.
- Informs all users that internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the [*system administrator / teacher / person responsible for URL filtering]*. Our system administrator(s) logs or escalates as appropriate to the technical service provider or LGFL helpdesk as necessary.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. Available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – police – and the LA.

Network management (user access, backup)

This school

- Uses individual, audited logins for all users - the London USO system.
- 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

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also *provide a different / use the same username and password* for access to our school's network.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual network log-in username.

- All pupils have their own unique username and password which gives them access to the Internet, *and (for older pupils) their own school approved email account*.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- 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. Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes.
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any “significant personal use” as defined by HM Revenue & Customs.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies, e.g., Borough email or Intranet, finance system, Personnel system etc.
- 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.
- Makes clear responsibilities for the daily back up of MIS and finance systems and other important files.
- 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.
- Uses our broadband network for our CCTV system and have had set-up by approved partners.
- Uses the dfe secure s2s website for all CTF files sent to other schools.

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX).
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network.
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school IT systems regularly with regard to health and safety and security.

Password Policy

- This school makes it clear that staff and pupils must always keep their password and class passwords private, must not share it with others and must not leave it where others can find it.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use <STRONG passwords for access into our Integris system.
- We require staff to change their passwords into the Integris, LGfL USO admin site, other secure system, every 90 days / twice a year

Electronic Communications

E-mail

- Pupils at this school use Microsoft O365
- Staff at this school use Microsoft O365 for all school emails
    - Both these systems are linked to the USO authentication system and are fully auditable, trackable and managed by lgfl on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.
- Email and Microsoft Teams Virtual learning (General Post and Show, Tell and Questions) are the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
  - Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, USO-FX and Egress systems are available from LGfL.

        - Internally, staff should use the school network, including when working from home when remote access is available via the Office 365 system.
- Pupils in Year 5 & 6 are restricted to emailing within the school and cannot email external accounts
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff
- Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- See also the social media section of this policy.

This school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
- Provides all pupils with an e-mail. Only year 5 &6 have access to this account.
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of lgfl-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language., Finally, and in support of these, lgfl webscreen2 filtering monitors and protects our Internet access to the World Wide Web.

Pupils:

Pupils are taught about the online safety and 'netiquette' of using e-mail, blogging, any sites which encourage communication both in school and at home i.e., they are taught:

- Not to give out their contact details unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer.
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.
- To 'stop and think before they click' and not open attachments unless sure the source is safe.
- That they should think carefully before sending any attachments.
- That they must immediately tell a teacher / responsible adult if they receive a communication which makes them feel uncomfortable, is offensive or bullying in nature.
- Not to respond to malicious or threatening messages.
    - Not to delete malicious of threatening communication, but to keep them as evidence of bullying.
    - Not to arrange to meet anyone they meet through communication without having discussed with an adult and taking a responsible adult with them.

- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff can only use the Microsoft O365 systems on the school system.
- Staff only use their school e-mail system for professional purposes.
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school-to-school transfer); Collect; USO-FX *or Egress.*
- Staff know that e-mails sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school 'house-style':
    - the sending of multiple or large attachments should be limited and may also be restricted by the provider of the service being used.
    - the sending of chain letters is not permitted.
    - embedding adverts is not allowed.
- All staff sign our school Agreement Form AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

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/Principal and Governors have delegated the day-to-day responsibility of updating the content of the website to [Communications Officer]. The site is managed by / hosted by the school's Communication Officer [Insert names/companies here; NB LGfL schools receive web hosting at no extra cost]. The school web site complies with the statutory DfE guidelines for publications.

Where other staff submit information for the website, they are asked to remember:

- 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. If in doubt, check with [Communications Officer]. There are many open-access libraries of high-quality public-domain images that can be used (e.g., pixabay.com for marketing materials – beware some adult content on this site). Pupils and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at curriculum.lgfl.net
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud Platforms

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

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

Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent). Parents and carers can at any time decide to withdraw their consent, but they should do so in writing.

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For a specific high-profile image for display or publication
- For social media

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.

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

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.

- 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.

- Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g., looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.
- We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).
- Pupils are taught about how images can be manipulated in their online-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Social Media

Staff, pupils' and parents' Social Media presence

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

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g., parent chats, pages or groups.

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 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don’t need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night’s sleep and productive teaching and learning at school the next day).

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.

- The school’s preferred system for social networking (twitter) will be maintained in adherence with the communications policy
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools’ preferred system for such communications.

School staff will ensure that in private use:

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

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

5. DEVICE USAGE

Personal Devices Including Wearable Technology

- Mobile phones brought into school are entirely at the staff member, parents' or visitors own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Student mobile phones are discouraged. Independent travellers in Y5 and 6 are allowed to bring mobile phones in for emergency use only. They must be handed in at the start of each day and returned at the end of the day. They are stored in the office for safe keeping. Mobiles must be turned off each morning. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the implementation of the school's Behaviour Policy, Safeguarding Policy and Exclusion Policy being implemented and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents/carers to pupils in emergencies
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent and in their pockets. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g., For contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member of staff.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

- 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.
- Where parents or students need to contact each other during the school day, they should do so only through the school's telephone.

Staff use of personal 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 are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

- If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy, then disciplinary action may be taken.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. 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.

Data security: Management Information System access and Data transfer

See data security policy

Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use / limited personal use within the framework of the acceptable use policy. All such use is monitored.
- **Home devices** are issued to some students. These are restricted to the apps/software installed by the school and may be used for learning and reasonable and appropriate personal use at home, but all usage may be tracked. The devices are filtered when in school and on home Wi-Fi connections.
- **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.
- **Parents** have no access to the school network or wireless internet on personal devices.

Trips / events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g., by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Searching and confiscation

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

Full details of the school's search procedures are available in the school Behaviour Policy

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

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

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

http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements. http://www.digitallyconfident.org/images/resources/first-line-information-supportHQ.pdf - page 23 onwards.

6. Protocol for Data Security- see data protection policy 6. Search and
Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

This policy is to be read in conjunction with the GDPR Suite of Policies which will outlines the school’s policies for: GDPR, Data Protection, CCTV and Photography.

Acceptable Use Agreement for Staff, Governors and Volunteers

Computing and the related technologies such as email, the internet and mobile phones are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of computing. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school online Safety coordinator.

- I understand the responsibilities listed for my role in the school's online safety policy and agree to abide by them
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the Computing system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on G2) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not browse, download, upload or send material that could be considered offensive or illegal.
- Images of pupils will only be taken (including on camera phones) and used for professional purposes and will not be distributed outside the school network without the permission of the parent/ carer.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will support and promote the school's Online-Safety policy and help pupils to be safe and responsible in their use of computing and related technologies.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate to the online-Safety co-coordinator.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I
  will keep any 'loaned' equipment up to date, using the school's recommended system.
- I will take full responsibility for my teacher loan laptop (as appropriate), for its security and safety and not leave it unattended at any time. Loss, theft or damage should be reported to the school as soon as possible.
- I will also take full responsibility for the security of the any computing resources (laptops, cameras, iPads). Loss, theft or damage should be reported to the school as soon as possible. Please do not lend any of these resources to anyone outside your year group. *Please note if a computing resource is lost, the school may charge you for replacing this.*

- I will ensure that any private social networking sites / blogs etc that I create or actively contribute too are not confused with my professional role and appropriate privacy settings put into place.
- I agree and accept that any laptop, USB stick, camera loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will not contact or attempt to contact any pupil or access their contact details (including their usernames/handles on different platforms) in any way other than for school-approved and school monitored activity, 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 online-Safety co-coordinator.
- I understand my duty to support a whole-school safeguarding approach and support the principle that 'safeguarding is a jigsaw' and that my concern might 'complete the picture' if I report it. Consequently, I will report any behaviour – staff or pupils - which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (DSL) or the Headteacher
- I agree to adhere to all provisions of the school Data Protection and GDPR policies at all times, and will ensure I do not access, nor attempt to access, store or share any data which I do not have express permission for.
- I will report any breaches or suspicions (by adults and children) in line with the school policy without delay.

To be completed by Governors/Staff/Volunteers

I have read and understood Tetherdown school's Online Safety policy and agree to follow this code of conduct and to support the safe use of Computing throughout the school

Laptop: Model
Make
Security Tag
Haringey Security Tag

iPad: Security Tag
Haringey Security Tag

Signature ……………………………………………… Date ……………………………………

Full Name ……………………………………………………………………….(printed)

Job title ……………………………………………………………………………..

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.)

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 either 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 the school may take action against me if I am involved in inappropriate behaviour on the internet and mobile devices.

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 Mobile Phones or watches linked to mobile data during the school day.

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.

(Only for reference: will take out later).
Searching and confiscation
In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher/Principal and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.
Full details of the school's search procedures are available in the school Behaviour Policy.

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.

Key Stage 1 Pupils Acceptable Use Online Safety agreement

TICK

I **KNOW** who my trusted adults are □

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

I am **KIND** and polite to everyone online □

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 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 □

Pupil name: ___________________________________

Class______________________

Date: __ __ _/_____/_____

Pupil Information Form Completed by Parents when they join the school.

<u>Photographs</u> Your child is likely to be photographed or filmed while engaging in the curriculum at Tetherdown. These photos or films may be subsequently used for display purposes, in publications such as our newsletter or on our website. Very occasionally they may be published externally, e.g., newspapers. We take care to ensure as far as possible that names are not attributable to individuals. 1. I give permission for my child to be photographed/filmed at school for: - a. Internal use (e.g., displays) b. Publications (e.g., newsletter and website) c. External publications (e.g., newspaper)	☐ Yes ☐ Yes ☐ Yes	☐ No ☐ No ☐ No
<u>Online Safety</u> As part of the school's ICT 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. 1. I give permission for my child to have access to and use the Internet, blogging, e-mail and other ICT facilities at school. 2. 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).	☐ Yes ☐ Yes	☐ No ☐ No
<u>Use of digital images, photography and video</u> 1. I understand the school has a clear policy on 'the use of digital images and video' and I support this. 2. I understand that the school will necessarily use photographs of my child or include them in video material to support learning activities.	☐ Yes ☐ Yes	☐ No ☐ No
<u>Social networking and media sites</u> 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. 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. 5. I understand that I will not take and then share online, photographs of other children (or staff) at school events without permission.	☐ Yes ☐ Yes ☐ Yes ☐ Yes ☐ Yes	☐ No ☐ No ☐ No ☐ No ☐ No

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/e- 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 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 of 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.