DOWNSVIEW PRIMARY SCHOOL

On-line Safety, Social Media, Devices and Acceptable Use Policy

Originator: Meghan Pugh
Approved: 16th May 2025
Revision Date: May 2026

Downsview Primary School
Biggin Way
Upper Norwood
London
SE19 3XE

Telephone: 020 8764 4611
Email: sec1@downsview.croydon.sch.uk
Webpage: www.downsview.croydon.sch.uk

On-Line Safety, Social Media, Devices and Acceptable Use Policy

Introduction

Key people / dates

Designated Safeguarding Lead (DSL) team	Meghan Pugh Emma Ricketts Caroline Hussey Nikki Gray Annette Nelson Alison Pemberton David Linton Allison Hearne-Reed
Online-safety Lead (if different)	Meghan Pugh
Online-safety / Safeguarding Link Governor	Andrew Walters
PSHCE/HRE Lead	Gemma Travers
Network Manager / other technical support	Croydon Education Partnership
Date this policy was reviewed and by whom	15th May 2025 - Meghan Pugh
Date of next review and by whom	May 2026 - Meghan Pugh
Associated policies	Safeguarding Policy, Behaviour Policy, Anti-bullying Policy, Staff Code of Conduct, Data Protection Policy, Data Retention Policy, IT Security Policy, Preventing Extremism and Radicalisation Safeguarding Policy

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 (KCSIE),' 2024, 'Teaching Online Safety in Schools' June 2019 (updated January 2023) and other statutory documents. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended, where necessary, during the year in response to developments in the school and local area. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Any changes to this policy will be updated on the School website.

How will this policy be communicated?

This policy can only impact upon practice if it is a regularly updated living document. It must be accessible to and understood by all stakeholders.

- Posted on the school website
- Available on the school network for staff
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors and pupils
- AUPs are issued to whole school community (to parents as part of their child's Admissions Form on entry to the school), with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms

Contents

Overview

Aims

This policy aims to:

- Deliver an effective approach to on-line safety, which empowers us to protect and educate the whole school community in its use of technology. This will be achieved by setting out expectations for all Downsview Primary & Nursery School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform.
- Have robust processes in place to facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
    - to minimise the risk of children and adults being exposed to inappropriate content on the web.
- Establish clear structures by which online misdemeanours will be treated and procedures to follow where there are doubts or concerns.
- To ensure that the school is in line with Statutory Requirements. This policy refers to statutory guidance on protecting children from radicalisation and reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying.

Further Help and Support

Internal school channels are always followed first, especially in response to incidents in line with our Safeguarding Policy. Our DSL will handle referrals to the local authority Single Point of Contact (SPOC) and normally the Headteacher will handle referrals to the LA Designated Officer (LADO).

Scope

This policy applies to all members of the Downsview community (including staff, governors, volunteers, contractors, pupils, parents/carers and visitors) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

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.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding Policy.

Acceptable use of the internet and devices in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (**Appendix 1**). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be used for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

The school will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Headteacher

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the Designated Safeguarding Officers and ensure that their 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 Officers 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, Designated Safeguarding Officers 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 or exploited.
- Ensure that there is a system in place to monitor and support staff 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.

Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL)

Key responsibilities:

The DSL at our school is the Headteacher and can delegate certain online-safety duties, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2023:

- "The Designated Safeguarding Lead should take lead responsibility for safeguarding and child protection (including online safety)."
- Ensure all staff understand this policy and are aware of the procedures that need to be followed in the event of an online safety incident or incidents of cyber bullying, and that these are logged in the same way as any other safeguarding incident using CPOMS.
- Ensure there is an effective approach to online safety that empowers all stakeholders, in their use of technology and establish mechanisms to identify, intervene in and escalate any incidents, where appropriate.
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area.
- Liaise with the Local Authority and work with other agencies in line with Working together to Safeguard Children 2023 (Updated in February 2024).
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.

- Work with the DPO and Governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- The team communicates regularly with the Designated Safeguarding Governor to discuss current issues, review any concerning incidents and issues that have been identified and shared with our IT provider to assess that the systems are in place are robust.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends via safeblog.lgfl.net and the LGfL safeguarding newsletter.
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Ensure DfE guidance on sexual violence and harassment included in Keeping Children Safe in Education 2024 is followed throughout the school and that staff adopt a zero-tolerance approach to this
- Facilitate training and advice for all staff:
    - all staff must read KCSIE Part 1 and all those working with children Annex A
    - it would also be advisable for all staff to be aware of Annex C (online safety)
- 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.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the Governors.

Governing Board, led by Safeguarding Link Governor

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2024:

- 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.
- Ensure an appropriate **senior member** of staff, from the school leadership team, is appointed to the role of DSL with **lead responsibility** for safeguarding and child protection (including online safety) with the appropriate status and authority and time, funding, training, resources and support.
- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with the OSL/DSL and incorporate online safety into standing discussions of safeguarding at governor meetings, including the monitoring of online safety concerns on CPOMS as provided by the DSL.
- Work with the DPO, DSOs 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 and understand Part 1 and Annex A of KCSIE; SLT and all working directly with children check that Annex C on Online Safety reflects practice in our school.

- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly aligned and considered as part of the overarching safeguarding approach.
- Ensure appropriate filters and appropriate monitoring systems are in place but be careful that 'overblocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure that children are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

All staff

Key responsibilities:

- 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) is.
- Read and understand Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 and Annex A are statutory for all staff, for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main Safeguarding Policy.
- Record online safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself.
- Sign and follow the staff Acceptable Use Policy and Code of Conduct.
- All staff must log off when finished working or leaving any device unattended. Staff should never share their passwords with other users, pupils or visitors.
- 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, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise.
- Whenever overseeing the use of technology (devices, the internet, new technology) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites' monitoring policies are in place.
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities, where appropriate), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting.
- Prepare and check all online sources and resources before using within the classroom.
- Remind and encourage pupils to follow their Acceptable Use Policy 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 in accordance with the school's Behaviour Policy.

- 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 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 safety issues.
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.
- Staff must always keep professional and private communications separate.

PSHCE (Safety, Healthy body, mind and spirit) Lead

Responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHCE 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 and technology 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 messaging within PSHE.

Computing and Technology Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the computing and technology curriculum in accordance with the national curriculum.
- 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 Policies.
- Maintain up-to-date documentation of the school's online security and technical procedures.

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:

- Look for opportunities to embed online safety in your subject, and model positive attitudes and approaches to staff and pupils alike.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within computing.
- Ensure subject specific planning also has an online-safety element.

Network Manager/Technician

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the DSL/OSL/DPO/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.
- 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.

Data Protection Team

Key responsibilities:

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

LGfL TRUSTnet Nominated contacts

Key responsibilities:

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

Governors, Volunteers and Contractors

Key responsibilities:

- Read, understand, sign and adhere to the school's Acceptable Use Policy (AUP).
- Report any concerns, no matter how small, to the DSL/OSL.
- Model safe, responsible and professional behaviours in their own use of technology.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the school's pupil Acceptable Use Policy.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials.
- Know what action to take if they, or someone they know, feels worried or vulnerable when using online technology.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's Acceptable Use Policies cover actions out of school, including on social media.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/Carers

Key responsibilities:

- Read and promote the school's Home School Agreement and read the pupil AUP and encourage their children to follow it (Appendix 1).
- Consult with the school if they have any concerns about their child's and others' use of technology.
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre (https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues)

- Parent factsheet - Childnet International (https://www.childnet.com/resources/parents-and-carers-resource-sheet)

External Groups, including Parent Associations and Visitors

Visitors and members of the community who use the school's IT systems or internet will be made aware of this Policy, where relevant, and be expected to read and follow it. Downsview uses a guest account for temporary restricted access to the internet and school network.

Key responsibilities:

- Any external individual/organisation will sign an Acceptable Use Policy prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection.
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting

negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.

Education and Curriculum

Educating Pupils about On-line Safety

A thorough and age appropriate e-safety curriculum is delivered to all pupils at Downsview to teach children how to stay safe when using computing technology in school or at home. This covers a range of skills and behaviours appropriate to their experience. The curriculum has been planned out to cover a broad range of online-safety aspects and prepare children for a digital world. The curriculum will review and remind students about their responsibilities through the pupil Acceptable Use Agreement(s), which differs between KS1 and KS2 (see Appendix 1).

Across the curriculum, it is ensured that pupils only use school-approved systems and work within appropriately secure / age-appropriate environments.

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information, including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

The school will also use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Educating Parents about On-line Safety

The school will raise parents' awareness of internet safety by running workshops and sharing information on our website, Newsletters, workshops and ClassDojo. This policy will also be published on the school website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher. The class teacher will then liaise with a member of the SLT, as well as the Headteacher.

ON-LINE SAFETY

Who is in charge of online safety?

The School's Designated Safeguarding Lead (DSL) is responsible for safeguarding and child protection, including online safety.

Cyber-bullying

Definition: Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Behaviour Policy and Anti-Bullying Policy).

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the one who has been harmed.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also shares information on cyber-bullying, via the school newsletter, to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member, in conjunction with the DSL or other member of the senior leadership team, to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school's complaints procedure.

Cyberbullying involving staff

All forms of bullying, including cyberbullying, are handled as a community issue for the whole school. It is important that we, as a school, take measures to prevent and tackle bullying among pupils, but it is equally important that schools make it clear that bullying of staff, whether by pupils, parents or colleagues, is unacceptable.

School leaders, teachers, school staff, parents and pupils all have rights and responsibilities in relation to cyberbullying and should work together to create an environment in which pupils can learn and develop and staff can have fulfilling careers free from harassment and bullying.

We will always aim to foster a good school-parent relationship, as it helps to create an atmosphere of trust that encourages parents to raise concerns in an appropriate manner. We will also offer support to parents on how to help their children engage safely and responsibly with social media, through workshops and advice. Part of this is making sure that parents and carers are aware and understand how to communicate with the school.

It is not acceptable for pupils, parents or colleagues to denigrate and bully school staff via social media in the same way that it is unacceptable to do so face to face. Schools should encourage all members of the school community, including parents, to use social media responsibly.

Parents have a right to raise concerns about the education of their child, but they should do so in an appropriate manner.

Staff who feel subject to cyber-bullying, should:

- Never respond or retaliate to cyberbullying incidents.
- Report incidents appropriately and seek support from your line manager or the SLT.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current pupil, parent or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments. If the perpetrator is a parent or significant member of the community, the person might become subject to the school's Persistent Complaints and Harassment Policy.
- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies, for example, the UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police as online harassment is a crime. Staff should never personally engage with cyberbullying incidents amongst other adults. Where appropriate, they should report incidents to the DSL/OSL and seek support.

Handling Online-safety Concerns and Incidents

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. Staff should also record any such concerns and incidents on CPOMS.

School procedures for dealing with online-safety can also be found in the following policies:

- Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy notices and consent forms for data sharing, image use)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow the school to deal with them quickly and sensitively through the school's Behaviour Policy.

Any suspected online risk or infringement should be reported to the DSL/OSL on the same day – where clearly urgent, it will be made by the end of the lesson.

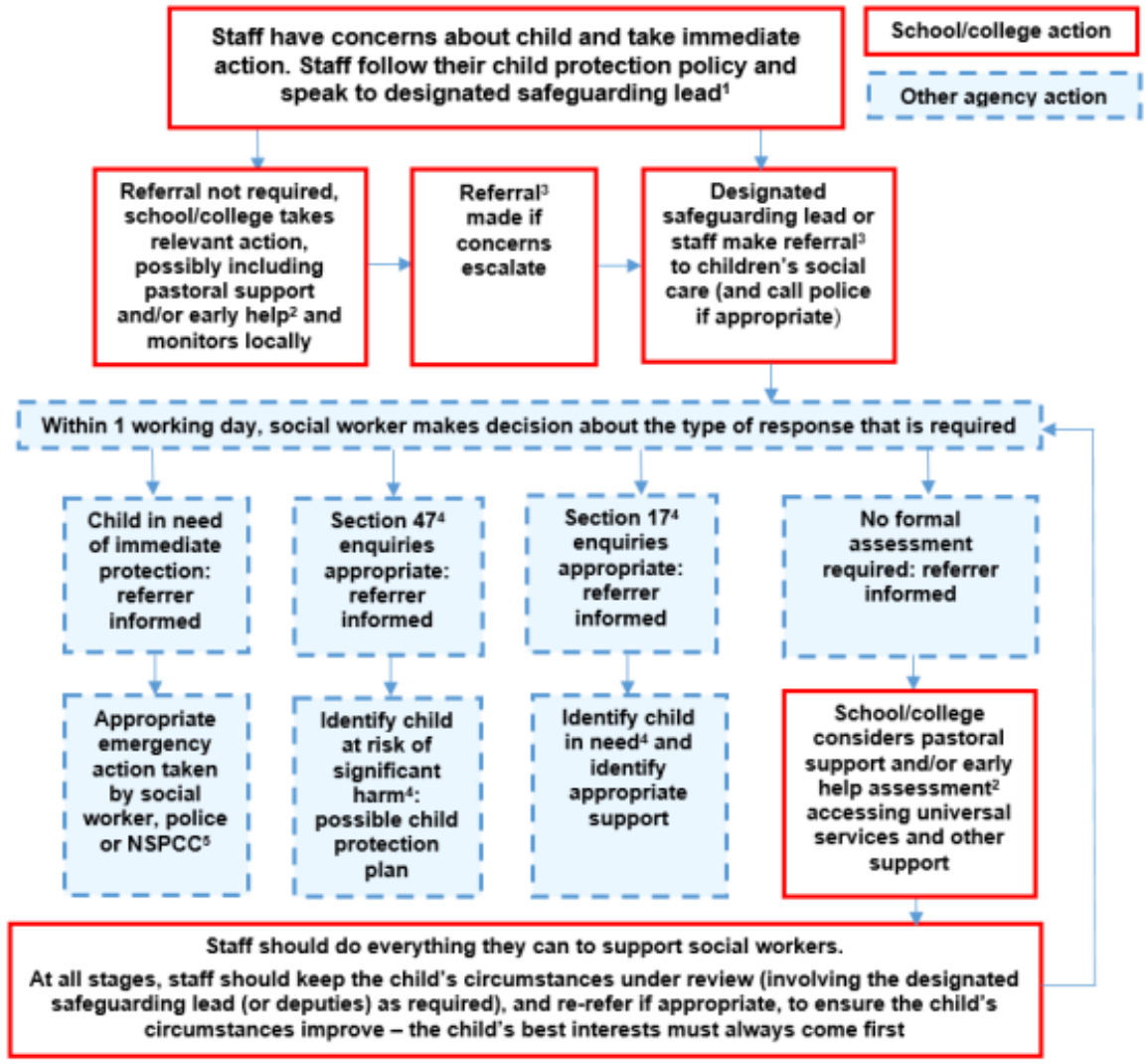
Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher, in which case the concern is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

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, 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).

Actions where there are concerns about a child

The following flow chart is taken from page 24 of Keeping Children Safe in Education 2024 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

Actions where there are concerns about a child



1 In cases which also involve a concern or an allegation of abuse against a staff member, see Part four of this guidance.
2 Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Working Together to Safeguard Children provides detailed guidance on the early help process.
3 Referrals should follow the process set out in the local threshold document and local protocol for assessment. See Working Together to Safeguard Children.
4 Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Working Together to Safeguard Children.
5 This could include applying for an Emergency Protection Order (EPO).

Sexting

Schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools.

There is a one-page overview for all staff (not just classroom-based staff) to read called: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759009/Overview_of_Sexting_Guidance.pdf, in recognition of the fact that it is mostly someone other than the DSL/OSL 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 to decide next steps and whether other agencies need to be involved: https://www.gov.uk/government/publications/sexting-in-schools-and-colleges

It is important that everyone understands that, whilst sexting is illegal, students or parents can come and talk to members of staff if they have made a mistake or had a concern 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) is now a criminal offence, as highlighted in Keeping Children Safe in Education 2024 and that students or parents can come and talk to members of staff if they have made a mistake or had a concern in this area.

Cyberbullying

Is it Conflict or Bullying?

Bullying incidents:

All incidents which are perceived to be bullying, however trivial, are investigated by the school. If, after investigation, the conclusion is that there was no bullying motivation, this information is recorded on CPOMs.

Possible outcomes once the bullying incident has been investigated:

A member of SLT will contact all parents and carers involved, initially inform them and also subsequently report back outcomes and actions.

The bully/bullies will receive a consequence as deemed appropriate by Senior Leadership and according to our Restorative Justice Approach. The severity of the consequence will depend on many aspects including:

- Age of those involved.
- Persistence/repetition of incidents.
- Knowledge of individuals past experiences, abilities and disabilities.
- Level of distress and harm caused.

- Context of the incident.

The consequences could include the following, but the list is not exhaustive and will be determined by the senior leader, on a case-by-case basis:

- Receiving a red card, which includes a letter to inform parents, in line with the school's Behaviour Policy.
- Making amends for the harm that has been done, such as writing a sincere letter of apology.
- "Give back in kindness", by taking on different responsibilities around the school, such as helping out in the dinner hall during lunch time.
- Playtimes and/or lunchtimes spent with a member of the team reflecting about their behaviour for a fixed period of time. This gives the person who has been affected time and space away from the child that caused the harm. This will be an opportunity for the child who caused the harm to reflect about their choices and how their choices affect other people.
- Restorative Justice conference.
- In serious cases or persistent cases, the Headteacher may make the decision to either internally exclude or do an external fixed term suspension.

The support from the Senior Leadership Team will continue until they feel the person who caused harm has taken responsibility and learned from their behaviour and the child who has been harmed feels safe.

Incident that deems to be Conflict:

Conflict can be defined where children have had a falling out and are unable to fix the issue without an adult's support. Where this is the case, the school will work with the children to try and resolve their issues through our Restorative Justice approach. Conflict is then monitored generally by the class teacher but could also be referred to the Learning Mentor.

Online bullying is treated like any other form of bullying and the school's Anti-bullying and Behaviour Policy should be followed for online bullying, which may also be referred to as cyberbullying. A copy of our Anti-bullying and Behaviour Policies can be found on our website.

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

Sexual Violence and Harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the guidance in Keeping Children Safe in Education 2024.

Staff fosters 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.

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 Policies 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.

Where pupils contravene these rules, the school's Behaviour Policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff Code of Conduct.

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.

Data Protection and Data Security

There are references to the relationship between data protection and safeguarding in key Department for Education documents, which the DPO and DSL will seek to apply.

'Keeping Children Safe in Education (2024)': https://www.gov.uk/government/publications/keeping-children-safe-in-education--2,

'Data Protection: a toolkit for schools (February 2023)': https://www.gov.uk/guidance/data-protection-in-schools/responsibilities and

'Information Sharing Advice for practitioners providing safeguarding services for children, young people, parents and carers (May 2024)': https://assets.publishing.service.gov.uk/media/66320b06c084007696fca731/Info_sharing_advice_content_May_2024.pdf. This quote from the latter document is useful for all staff:

'Data protection legislation (the Data Protection Act 2018 (the DPA 2018) and UK General Data Protection Regulation (UK GDPR)) does not prevent the sharing of information for the purposes of safeguarding children, when it is necessary, proportionate and justified to do so. In fact, data protection legislation provides a framework which enables information sharing in that context. The first and most important consideration is always whether sharing information is likely to support the safeguarding of a child. The ICO's A 10 step guide to sharing information to safeguard children summarises data protection considerations when sharing personal information for child safeguarding purposes: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/a-10-step-guide-to-sharing-information-to-safeguard-children/'

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Data Protection Policy.

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

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

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of USO-FX / Egress to encrypt all non-internal emails is compulsory for sharing pupil data.

The School's IT Security Policy covers all data protection aspects relating to data security.

School Network

Staff are only provided with access to authorised areas of the school network through their unique user ID and password to the school network. Downsview requires staff to log-out of systems when leaving their computer.

All servers are in lockable locations and managed by DBS-checked staff.

Details of all school-owned hardware are recorded on the school's asset register. Software is monitored across devices to ensure that it is in line with school policies.

ICT equipment will only be disposed of or recycled when hard drives are wiped clear of all school data.

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. The DSL oversees logging the behaviour and safeguarding issues related to online safety, using CPOMs.

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called School Protect from LGfL, which is made specifically to protect children in schools. This blocks sites which fall into categories, e.g. adult content, race hate, gaming, this is applied to every device in the school with different policies applied to staff and pupils. Securly filtering is also used on the pupil Chromebooks and offers enhanced filtering to meet the safeguarding and KCSIE guidelines. All changes to the filtering policy are logged and only available to staff with approved web filtering management status.

Network health is checked and maintained through the use of Sophos anti-virus software through LGFL. The following solutions are also used by the school: USO sign on for LGfL services, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management.

Electronic Communications

Email

The school uses LGFL Staffmail or its chosen e-mail messaging provider for sending emails.

The LGFL Staffmail system is linked to the USO authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Emails to parents 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 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 used.
    - Internally, staff should use the school network, including when working from home using the school's remote access.
- 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.
- Staff are NOT allowed to use the email system for personal use and should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times.
- Emails using inappropriate language, images, malware or to adult sites will be blocked and not arrive at their intended destination.

School Website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Headteacher/Senior Administration Officer. The site is managed by / hosted by Primarysite.

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission. If in doubt, check with the Headteacher.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

Cloud Platforms

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to also enhance teaching and learning.

This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies' (April 2019) and 'Meeting Digital and Technology Standards in Schools and Colleges' (updated May 2024): https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cloud-solution-standards-for-schools-and-colleges.

Uploading of information onto the school's chosen online learning space is shared between different staff members according to their responsibilities, e.g. all class teachers upload information in their class areas; documents uploaded to the school's online environment will only be accessible by members of the school community and are solely related to children's work.

In school, pupils are only able to upload and publish within school approved 'Cloud' systems to save any school related document.

Staff are prohibited from using any USBs, external hard drives or personal cloud storage as this can cause a risk to the system or transfer sensitive data. All staff have the facility to remotely access the school network, which can be used to transfer appropriate data and information securely.

For online safety, basic rules of good password protection apply, and training can help to keep staff and pupils safe.

The following principles apply:

- Privacy Notices inform parents, staff and stakeholders when and what sort of data is stored in the cloud.
- The Headteacher 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 assessment) and parental permission is sought, where required.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake.
- Two-factor authentication is used for access to staff or pupil data.
- Pupil images/videos are only made public with parental consent.
- Only school-approved platforms are used by pupils 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 and for how long.

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.

Parents may be given consent to take photographs and videos of their children in situations such as Family Assemblies and Sports Day. However, a member of staff will give permission prior to the event, if allowed to do so. Under no circumstance should these images be posted on social media as they may include children whose parents have refused consent for images to be used on these platforms.

Staff and parents are reminded 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.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them.

Photos are stored on the school network, Website, Googledrive, Classdojo and the school's Early Years Assessment software package, in line with the retention schedule of the school Data Protection Policy.

CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission, unless required to do so by law in the with the school's CCTV Policy

Social Media

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online. Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

The DSL/OSL is responsible for managing our Twitter account and checking our Google reviews. They follow the guidance in the LGfL / Safer Internet Centre online-reputation management document https://static.lgfl.net/LgflNet/downloads/online-safety/LGfL-OS-Advice-Online-Reputation-Managment-for-Schools.pdf .

Social media (including all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use Policies which all members of the school community are expected to comply with, 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.

Parents and Pupils

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school's Complaints Procedure, which can be found on the school website, 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.

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms, wherever possible, and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise.

Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when.

Email and ClassDojo are the official electronic communication channels between parents and the school.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control. In the reverse situation, however, staff must not follow such public pupil accounts.

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

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

Staff Use of Social Media and Messaging Apps

Staff should be mindful, that when using social media accounts and Messaging Apps, it is good practice to remember the following:

- Nothing is completely private.
- Nothing can be completely deleted.
- Staff are not permitted to have parents, carers or children of Downsview as friends or personal contacts in any social media and/or messaging apps, e.g WhatsApp, unless agreed to by the Headteacher.
- Staff are not to engage in any discussion on-line with parents, carers or children or to engage in discussions about named parents, carers or children using messaging apps, which are outside formal channels. Whilst some parents may feel that it is quicker or easier to raise concerns about their child via social media/messaging apps, staff should not engage in correspondence via social media platforms.
- Personal opinion should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute.
- Employees must not use social media to express personal viewpoints of School Policy or Headteacher or Governor decisions.
- Staff should regularly check their personal social media profiles to minimise risk of loss of personal information and to ensure that content that is public, is appropriate.
- Staff must maintain a clear understanding of this policy and agree and adhere to the terms on Acceptable Use on the school's ICT systems and the internet.
- Employees must limit their use of social media on their own equipment to their official break times, such as their lunch break. They should ensure that use of social media does not interfere with their

other duties. The School understands that employees may wish to use their own computers or devices, such as laptops, mobiles and hand-held devices, to access social media websites while they are at work; however, any access must adhere to this Policy.

Monitoring Use of Social Media during Work Time

Communications using School facilities may be intercepted, recorded and monitored for business use and where appropriate for the detection and prevention of crime. This includes, but is not limited to, telephone calls, internet use, email and post.

The School considers that valid reasons for checking employees' internet usage include suspicions that employees have:

- been using social media websites when they should be working; or
- acted in a way that is in breach of the rules set out in this Policy.

The School reserves the right to retain information that it has gathered on employees' use of the internet. Employees must note that the majority of social media websites are prohibited through the school's filtering.

Using Social Media and Messaging Apps in the Personal Life of Staff

The School recognises that many employees make use of social media and messaging apps, e.g. WhatsApp, in a personal capacity. While they are not acting on behalf of the School, employees must be aware that they can damage the reputation of the organisation if they are recognised as being one of our employees and are posting text, images (or both) that could be deemed inappropriate. Staff should be aware the sharing of personal data regarding an individual parent, pupils or work colleague constitutes data sharing under data protection legislation and could be requested in the event of the school receiving a Subject Access Request under the Data Protection Act 2018.

Employees should use their professional judgment when posting on social media and should review their social media history to ensure that there are no inappropriate historic posts or pictures, which could damage their professional reputation.

Employees should review their social network accounts, particularly the content and privacy settings in place.

Even if an employee does not specifically name the School on social media, it is likely that some viewers will know whom they are employed by and, as such, communications still have the potential to bring the organisation into disrepute.

Employees are allowed to say that they work for the School, which recognises that it is natural for its staff to sometimes want to discuss their work on social media. However, the employee's online profile (for example, the name of a blog or a Twitter name) must not contain the School's name.

If employees do discuss their work on social media (for example, giving opinions on their specialism or the education sector), they should make it evident that any view expressed is their own.

Photographs of pupils and school activities must not be uploaded or shared by employees through social media.

Any communications that employees make in a personal capacity through social media should be completed with professional judgment and must not:

- have the potential to bring the School into disrepute, for example:
  - by criticising or arguing with parents, colleagues or rivals;
  - by making defamatory comments about individuals or other organisations or groups; or
  - by posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example:
  - by sharing confidential information about an individual (such as a colleague or pupils) or the School; or
  - by discussing the School's internal workings (such as future plans that have not been communicated to the public, parents or pupils);
- breach copyright, for example:
  - by using someone else's images or written content without permission;
  - by failing to give acknowledgement where permission has been given to reproduce something; or
- do anything that could be considered discriminatory, bullying or harassment of an individual or group, for example:
  - by making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - by using social media to bully or criticise another individual (such as an employee of the organisation); or
  - by posting images that are discriminatory or offensive, or links to such content.

Disciplinary Action over Social Media Misuse

Misuse of social media websites and/or apps can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against the employee and/or the School. It may also cause embarrassment to the School.

In particular, uploading, posting, forwarding or posting a link to any of the following types of material on a social media website or via email, whether in a professional or personal capacity, will amount to gross misconduct:

- pornographic material;
- a knowingly false or defamatory statement about any person or organisation;
- material which is potentially offensive, obscene, discriminatory, derogatory or may cause embarrassment to the School, or its staff;
- online bullying of colleagues;
- promotion of radicalisation and extremism;
- confidential information about the School, any of our staff or pupils;
- any other statement which is likely to create any liability;

- material which breaches copyright or other intellectual property rights, or which invades the privacy of any person.

Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with its Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the investigation. If necessary, such information may be handed to the police in connection with a criminal investigation.

Any such action will be addressed under the school's Disciplinary Procedure and is likely to result in summary dismissal.

Cyber Bullying

Staff should never personally engage with cyberbullying incidents. Where appropriate, they should report incidents to the DSL/OSL.

Staff should keep any records of the abuse – text, e-mails, voicemail, website or instant message. If appropriate, screen prints of messages or web pages could be taken and time, date and address of site should be recorded, though care needs to be taken when copying certain images.

Staff should inform the SLT or Headteacher of incidents at the earliest opportunity.

Where the perpetrator is known to be a current pupil or colleague, the majority of cases will be dealt with most effectively under the relevant school disciplinary procedure.

Where a potential criminal offence has been identified, and reported to the police, the school will ensure that any internal investigation does not interfere with police inquiries.

Where pupils are found to have made unfounded, malicious claims against staff members, relevant and appropriate disciplinary processes will be applied with rigour, as is the case in relation to physical assaults.

Device Usage

Personal mobile devices which are brought into school are at the owners' own risk. The school accepts no responsibility for the loss, theft or damage of any mobile device brought onto the premises.

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

Pupils bringing mobile phones into school

The school accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. However, the school strongly discourages children from bringing in mobile devices, unless absolutely necessary. Downsview is a 'smartphone free' school. This means that children in Years 5 and 6, who are allowed to bring phones to school, will not be allowed to bring in smartphones. Mobile phones of pupils in Year 5 must be kept in the school office until they go home. If the child is in Year 6 then the phones are stored in the Year 6 safe. Even though the phones are kept in the office or Year 6 safe, the school do not accept responsibility for any lost or stolen phones.

Any use of mobile devices in school by pupils must be in line with the Acceptable Use Policy (see Appendix 1).

Any breach of the Acceptable Use Agreement by a pupil may trigger sanctions in line with the school Behaviour Policy, which may result in the confiscation of their device.

Appropriate use of mobile devices/phones by staff

The school allows staff to bring their mobile phones or devices into school. Personally owned mobile devices should not automatically synchronise with any school endorsed system, however there are occasions when the Headteacher will approve the use of personal mobile phones for dual authentication purposes. In the case of a personal device accessing school email, members of staff must ensure that appropriate steps are in place to protect personal data by using secure pin codes or passwords. Failure to do so could result in disciplinary action, a breach notification and/or a fine imposed under General Data Protection Regulation.

All staff who work directly with children should leave their mobile phones on silent and only use them in private staff areas during school hours. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

School phones (landline and mobile) must be used for all school purposes including emergency calls. When children undertake a school trip or journey, the school's mobile phone should be used. If more phones are needed, the staff accompanying the group may use their own phone, but for the limited purpose of contacting the other adults in the group, the school office, or the venues being visited or an emergency number if needs be.

Personal mobile phone technology may not be used to take photographs or videos. Only digital devices that belong to the school should be used to record visual information within the consent criteria guidelines of the school.

Safe and appropriate use of mobile phones by volunteers, contractors and governors

Upon their initial visit governors, volunteers and visitors are given information on the Inventry system regarding the use of mobile phones in school. If they wish to make or take an emergency call, they may use the school's phones. Governors, volunteers or visitors are not permitted to take photographs or recordings of the children on their mobile phones, unless prior permission is sought by the Headteacher.

Safe and appropriate use of mobile phones by Parents

Parents are asked not to use their mobile phones when on the school site. However, if parents/carers wish to take photos or videos at school events, these should be kept for family use only and not shared in the public domain, including social media, as some of our parents/carers have not consented for their child's images to be shared.

How the School will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, according to the Acceptable Use Policy (Appendix 1), action will be taken. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member or governor misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff/governor Code of Conduct and/or Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents, which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Network / internet access on school devices

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of Acceptable Use, as set out in Appendix 1.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If staff have any concerns over the security of their device, they must seek advice from the Business Manager, who will seek advice from the IT support company, as appropriate. Work devices must be used solely for work activities.

Volunteers, contractors, governors can access the guest wireless network but have no access to networked files/drives. Parents have no access to the school network or wireless internet on personal devices and the Guest login credentials for the school wireless network should not be shared with parents

Trips / Events away from school

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with parents. 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 accessing a teacher's private phone number. This can be done by inputting 141 in front of the phone number they are calling, which will temporarily hide their mobile number from the recipient of the call. No parent/volunteer is to use their own mobile phone during the duration of the trip, including taking pictures.

Searching and Confiscation

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

Online Safety Concerns & Incidents

The school will take all reasonable precautions to ensure children are taught about online safety and how to keep themselves and their information safe. Pupils are given information about infringements and possible sanctions through specific teaching sessions, circles, assemblies etc. Staff are given information about infringements and possible sanctions through policy, training etc. The class teacher acts as first point of contact for any incident, which should be investigated in accordance to our Behaviour Policy and then reported on CPOMs. Any concern about staff misuse is always referred 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).

At Downsview, there is strict monitoring and application of this Policy and a differentiated and appropriate range of sanctions.

All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's Behaviour Policy.

It may be deemed appropriate that parents/carers are specifically informed of online safety incidents involving young people, for whom they are responsible. The police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law. Support is actively sought from other agencies, as needed (i.e. the Local Authority, LGfL, UK Safer Internet Centre helpline, Child Exploitation and Online Protection, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues.

We will immediately refer any suspected illegal material to the appropriate authorities, including the Police, with the LA also being informed. Monitoring and reporting of online incidents that occur contributes to developments in policy and practice in online safety within the school.

Appendices

1. Acceptable Use Policies (AUPs) for:
    - Pupils – KS1 & KS2
    - Staff and Volunteers
    - Governors
    - Contractors
    - Parents (Home-School agreement)

Appendix 1

Downsview KS1 Acceptable Use Policy 2024

Think before you click

S	**I will only use the Internet with an adult**
A	**I will only click on icons and links when I know they are safe**
F	**I will only send friendly and polite messages**
E	**If I see something I don't like on a screen, I will always tell an adult**

My Name:

My Signature:

Downsview KS2 Acceptable Use Policy 2025/26

These rules will keep me safe and help me to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will use the school's computers and equipment sensibly. Look after it and make sure it is stored securely when I have finished using it.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.

I have read and understand these rules and agree to them.

Signed: _____ *Date:* _____

Acceptable Use Agreement: All Staff and Volunteers

AUP review Date	**September 2025**
Date of next Review	**September 2026**
Who reviewed this AUP?	**ICT Leader**

What is an AUP?

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

This AUP is reviewed annually, and staff and volunteers will be asked to sign it upon entry to the school, annually at the start of the academic year and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal/professional obligations and it is imperative that all parties understand that online safety is part of safeguarding, as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy, as detailed in the school's Online Safety, Social Media, Devices and Acceptable Use Policy.

All staff, governors and volunteers should read the school's Online Safety, Social Media, Devices and Acceptable Use Policy. If you have any questions about this AUP or our approach to online safety, please speak to the school's Designated Safeguarding Lead/Headteacher.

What am I agreeing to?

This AUP covers use of all digital technologies in school and remotely: i.e. email, Internet, network resources, learning platforms, software, communication tools, equipment and systems.

- I have read and understood the school's Online Safety, Social Media, Devices and Acceptable Use Policy and IT Security Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with these policies without delay.
- I understand the responsibilities listed for my role in the school's Online Safety, Social Media, Devices and Acceptable Use Policy. This includes promoting online safety as part of a whole school approach in line with the HRE curriculum, as well as safeguarding considerations when supporting pupils remotely.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead.
- I understand that school systems and users are protected by security, monitoring and filtering services and that all Internet and network traffic/usage is logged and this information can be made available to the Headteacher / Designated Safeguarding Lead/ authorised staff members on their request.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:
  - not sharing other's images or details without permission
  - refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
- I understand that the school's Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. I agree to adhere to all provisions of the school's Data Protection Policy at all times, whether or not I am on site or using a school device, platform or network, and will ensure I do not access, attempt to access, store or share any data which I do not have express permission for.
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Board.
- I will follow 'good practice' advice in the creation and use of my password. I will protect my passwords/logins and other access, never share credentials and immediately change passwords and notify the Headteacher if I suspect a breach; this includes passwords to any personal devices where used to access school data.
- I will not allow unauthorised individuals to access my school email address / the Internet / the school network, or other school systems, or any Local Authority (LA) system I have access to without the Headteacher's prior consent.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's IT Security Policy and Data Protection Policy.
- I will not engage in any online activity that may compromise my professional responsibilities. I will ensure, where used, I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I will only use the approved email system(s) for any school business.
  This is currently: *LGfL StaffMail*
- I will only use school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business. For more details, read the school's Online Safety, Social Media, Devices and Acceptable Use Policy.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the ICT Leader or School Business Manager.
- I will only use safe and appropriately licenced software, respecting licensing, intellectual property and copyright rules at all times. I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.
- I will not download any software or resources from the Internet without the prior consent of the School Business Manager who will conduct a Data Protection Impact Assessment prior to approving the software/resources.
- I will not store school-related data on personal devices, USBs, personal storage or cloud platforms. If access to work related content is required, then I will use either remote access or school provided cloud systems.
- I will not use personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos on personal devices or at home.

- I will only use school approved equipment, networks or cloud systems for storage, editing or transfer of digital images / videos of children and staff.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities.
- I will only access school resources remotely using the school approved systems.
- I will alert Downsview's ICT Leader and/or the Designated Safeguarding Lead/ appropriate senior member of staff if I feel the behaviour of any user of the school's IT systems may be a cause for concern.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- *Staff that have a teaching role only:* I will embed the school's Online Safety, Social Media, Devices and Acceptable Use Policy into my teaching.

Acceptable Use Policy (AUP): Agreement Form

All Staff and Volunteers

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety, Social Media, Devices and Acceptable Use and IT Security Policies.

I understand failure to comply with this Acceptable Use Agreement and/or of the school's Online Safety, Social Media, Devices and Acceptable Use Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Signature Date

Full Name (printed)

Job title / Role

Authorised Signature (Headteacher / Deputy)

I approve this user to be set-up on the school systems relevant to their role.

Signature Date

Full Name (printed)

Acceptable Use Agreement: Governors 2024

AUP review Date	**September 2025**
Date of next Review	**September 2026**
Who reviewed this AUP?	**ICT Leader**

What is an AUP?

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

This AUP is reviewed annually and Governors will be asked to sign it upon entry to the school, annually at the start of the academic year and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal/professional obligations and it is imperative that all parties understand that online safety is part of safeguarding, as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy, as detailed in the school's Online Safety, Social Media, Devices and Acceptable Use Policy.

All staff, governors and volunteers should read the school's Online Safety, Social Media, Devices and Acceptable Use Policy. If you have any questions about this AUP or our approach to online safety, please speak to the school's Designated Safeguarding Lead/Headteacher.

What am I agreeing to?

This AUP covers the use of all digital technologies in school and remotely: i.e. email, Internet, intranet, network resources, learning platforms, software, communication tools, equipment and systems.

- I will follow the school's Online Safety, Social Media, Devices and Acceptable Use and IT Security Policies.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead.
- I will only use the school's digital technology systems for professional purposes or for uses deemed 'reasonable' by the Headteacher and Governing Board.
- I will not allow unauthorised individuals to access the school Internet or other school systems, or any Local Authority (LA) system I have access to without the Headteacher's prior consent.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's IT Security Policy and Data Protection Policy.

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that the email system I use for any school business is password protected and will not share the password. I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it immediately.
- I will not reveal my password(s) to anyone, this includes personal devices where used to access school data.
- I will only use school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of, inappropriate materials or filtering breach to the ICT Leader or School Business Manager.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos on personal devices or at home, in my capacity as a school governor. As a Parent Governor (where applicable) I understand that if taking photos or video recordings of any school event on a personal device, these should please be kept for family use only and will not be shared in the public domain, including social media.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely, so as not to compromise my professional role.
- I understand that the school's Data Protection Policy requires that any information seen by me with regard to staff or pupil will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I understand that all Internet and network traffic / usage can be logged and this information can be made available to the Designated Safeguarding Lead/Headteacher on their request.
- I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

Acceptable Use Policy (AUP): Agreement Form for Governors 2024

User Signature

I agree to abide by all the points set out in the Acceptable Use Agreement.

I undertake to be a 'responsible digital technology user'.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Online Safety, Social Media, Devices and Acceptable Use and IT Security Policies.

Signature …….. Date…….

Full Name (Please print)