



# **WANSTEAD HIGH SCHOOL**

## **Online Safety Policy**

**Approved by: Governing Body**

**Last reviewed on: October 2021**

**Next review due by: June 2022**

## Introduction

### Key People

Designated Safeguarding Lead (DSL) & Online Safety Lead	Mr J Gharu
Online Safety / Safeguarding Link Governor	Ms Y MacCallum
PSHE/RSHE Lead	Ms F Mannan
Network Manager / other technical support	Computer Talk
Date this policy was reviewed and by whom	Mr J Gharu June 2021
Date of next review and by whom	Mr J Gharu June 2022

### What is this Policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

### Who is in charge of Online Safety?

The named online safety lead is Mr Jason Gharu; the designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).

The LGfL DigiSafe 2018 pupil survey of 40,000 students identified an increase in distress caused by, and risk from, content. For many years, online-safety messages have focussed on 'stranger danger', i.e. meeting strangers online and then meeting them face to face (contact). Whilst these dangers have not gone away and remain important, violent or sexual content is now prevalent – sending or receiving, voluntarily or coerced. Examples of this are the sharing of violent and sexual videos, self-harm materials, and coerced nudity via live streaming. Contact and conduct of course also remain important challenges to address.

## Online Safety

An effective approach to online safety empowers the school to protect the whole school community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

Schools and colleges should have appropriate filters and monitoring systems in place to limit children's exposure to online risks. Settings should also ensure they have appropriate security procedures in place to safeguard their systems.

The breadth of incidents classified within online safety is considerable, but can be categorised into four areas of risk. These areas are a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all four.

- **content:** being exposed to illegal, inappropriate or harmful material: for example, pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users: for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

## How will this policy be communicated?

It will be communicated in the following ways:

- Posted on the school website.
- Available on the internal staff network/drive.
- Integral to safeguarding updates and training for all staff (especially in September refreshers).
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, students and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review.

## Overview

### Aims

This policy aims to:

- Set out expectations for all Wanstead High School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform.
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy).

### Further Help and Support

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

Beyond this, [reporting.lgfl.net](https://www.reporting.lgfl.net) has a list of curated links to external support and helplines for both students and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

### Scope

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

## **Roles and Responsibilities**

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, students, 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.

### **Acting Headteacher – Mr J Gharu**

#### **Key responsibilities:**

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships.
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles.
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident.
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of students, including risk of children being radicalised.
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures.
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety.
- Ensure the school website meets statutory requirements (see appendices for website audit document).

## Designated Safeguarding Lead / Online Safety Lead – Mr J Gharu

### Key responsibilities:

- “The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety).”
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL’s clear overarching responsibility for online safety is not compromised.
- Ensure “An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.”
- “Liaise with the local authority Redbridge and work with other agencies in line with Working together to safeguard children.”
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns.
- Work with the Headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Stay up to date with the latest trends in online safety – the new LGfL DigiSafe pupil survey of 40,000 students may be useful reading (new themes include ‘self-harm bullying’ and getting undressed on camera).
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see [safelog.lgfl.net](http://safelog.lgfl.net) for examples or sign up to the [LGfL safeguarding newsletter](#).
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework ‘Education for a Connected World’) and beyond, in wider school life.
- 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, but also including hard-to-reach parents.
- Liaise with school technical, pastoral, and support staff as appropriate.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss how filtering and monitoring.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Oversee and discuss ‘appropriate filtering and monitoring’ with governors (is it physical or technical?) and ensure staff are aware.
- Ensure the 2018 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- 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)

- cascade knowledge of risks and opportunities throughout the organisation
- [cpd.lgfl.net](http://cpd.lgfl.net) has helpful CPD materials including PowerPoints, videos and more

## **Governing Body, led by Online Safety / Safeguarding Link Governor – Ms Y MacCallum**

### **Key responsibilities:**

- Approve this policy and strategy and subsequently review its effectiveness, e.g. by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) [Online safety in schools and colleges: Questions from the Governing Board](#).
- Ensure an appropriate senior member of staff, from the schools 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 online-safety co-ordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised.
- Work with the DPO, DSL and Headteacher to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated, in line with advice from the local three safeguarding partners, integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at [cpd.lgfl.net](http://cpd.lgfl.net).
- "Ensure appropriate filters and appropriate monitoring systems are in place [but...] be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding". LGfL's appropriate filtering submission is [here](#).
- "Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum. Consider a whole school to online safety [with] a clear policy on the use of mobile technology." In line with 'Teaching Online Safety in Schools 2019'.

## 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 the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is Mr Jason Gharu.
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A 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.
- Follow the staff acceptable use policy and code of conduct/handbook.
- 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 (which have a unique value for students).
- Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).
- To carefully supervise and guide students when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
- Prepare and check all online source and resources before using within the classroom.
- Encourage students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL/OSL of new trends and issues before they become a problem.
- Take a zero-tolerance approach to bullying and low-level sexual harassment.
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know.
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe [pupil survey](#) of 40,000 students (new themes include 'self-harm bullying' and getting undressed on camera).
- 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. More guidance on this point can be found in this [Online Reputation](#) guidance for schools.



## **PSHE Lead – Ms F Mannan**

### **Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their students' lives."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that students 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 / RSHE.

## **Computing Lead – Mr B Alom**

### **Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

## **Curriculum Team Leaders**

### **Key responsibilities:**

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, and model positive attitudes and approaches to staff and students alike.
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online-safety element.

## Network Management / Technician – Computer Talk

### Key responsibilities:

- As listed in the ‘all staff’ section, plus:
- Keep up to date with the school’s online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL nominated contact to ensure that school systems and networks reflect school policy.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Support and advise on the implementation of ‘appropriate filtering and monitoring’ as decided by the DSL and senior leadership team.
- Maintain up-to-date documentation of the school’s online security and technical procedures.
- To report online-safety related issues that come to their attention in line with school policy.
- Manage the school’s IT Infrastructure, including but not limited to, it’s networks, operating systems, software and devices. As well as implementing suitably strict password policies, with systems in place for detection of misuse and malicious attacks, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- As an LGfL school ensure that the school takes advantage of the following solutions which are part of the LGfL’s broadband package: Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress, Meraki Mobile Device Management and CloudReady/NeverWare.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line to DSL or Ms D Cini.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

## Data Protection Officer (DPO) – Mr A Patel

### Key responsibilities:

- GDPR information on the relationship between the school and LGfL can be found at [gdpr.lgfl.net](https://gdpr.lgfl.net); there is an LGfL document on the general role and responsibilities of a DPO in the ‘Resources for Schools’ section of that page.
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents ‘Keeping Children Safe in Education’ and ‘Data protection: a toolkit for schools’ (August 2018), especially this quote from the latter document:
- “GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children’s Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

**The Data Protection Act 2018 introduced ‘safeguarding’ as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When

Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children.”

- 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. [gdpr.lgfl.net](http://gdpr.lgfl.net).
- 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.
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at [gdpr.lgfl.net](http://gdpr.lgfl.net).

## **Volunteers and Contractors**

### **Key responsibilities:**

- Read, understand, sign and adhere to an acceptable use policy (AUP).
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP.
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology.

## **Students**

### **Key responsibilities:**

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually.
- 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, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it.
- Consult with the school if they have any concerns about their children's and others' use of technology.
- Promote positive online safety and model safe, responsible 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, students or other parents/carers.

NB: the LGfL DigiSafe survey of 40,000 primary and secondary students found that 73% of students trust their parents on online safety

## **External groups including parent associations**

### **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, students or other parents/carers.

## **Education and Curriculum**

The following subjects have the clearest online safety links:

- PSICHE
- Relationships education, relationships and sex education (RSE) and health
- Computing

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

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

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

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

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

### **Handling online safety concerns and incidents**

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

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

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

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Risk Assessment / Policy
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

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

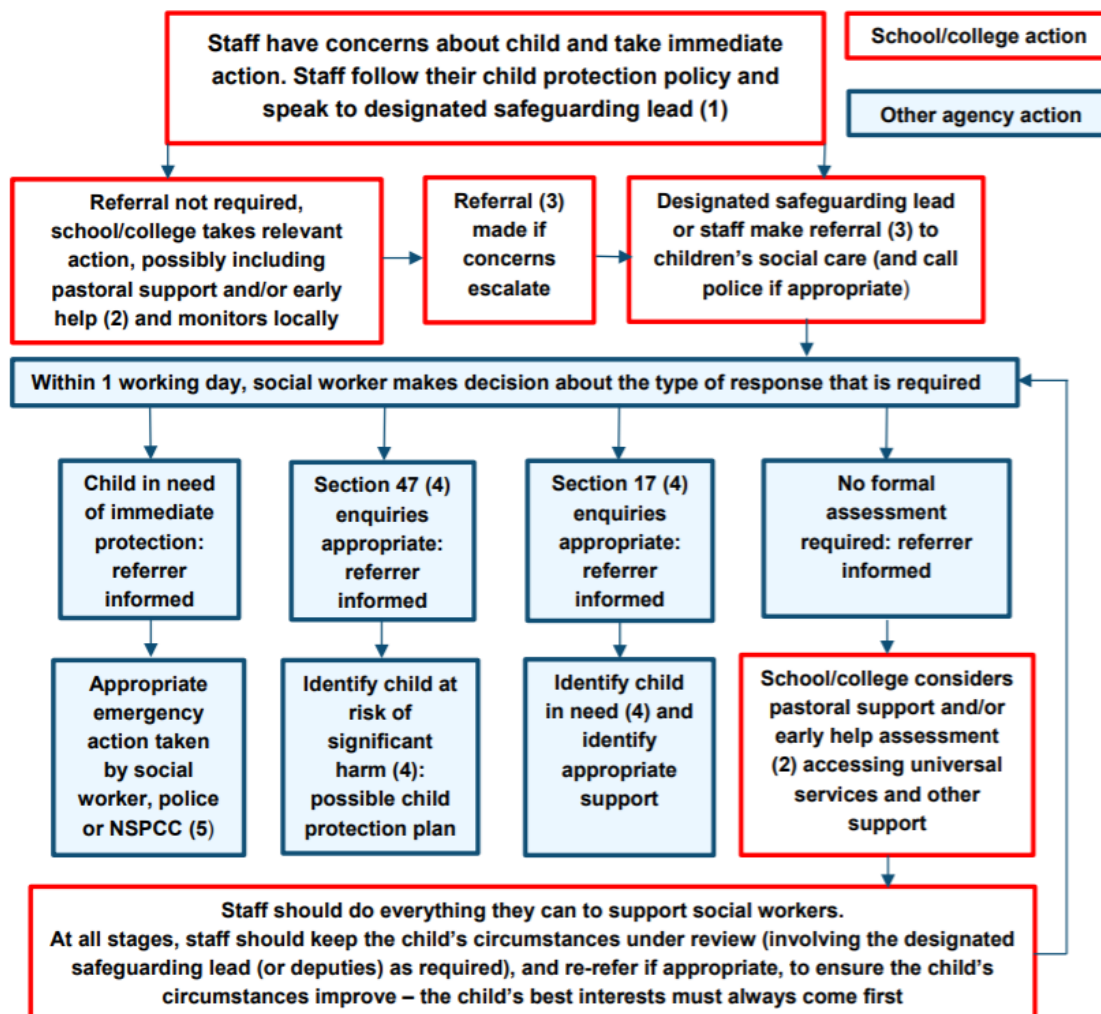
Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

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

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 students 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).

## Actions where there are concerns about a child

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2019 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



(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. Chapter one of [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. Chapter one of [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 Chapter one of [Working Together to Safeguard Children](#).

(5) This could include applying for an Emergency Protection Order (EPO).

## Sexting

All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

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

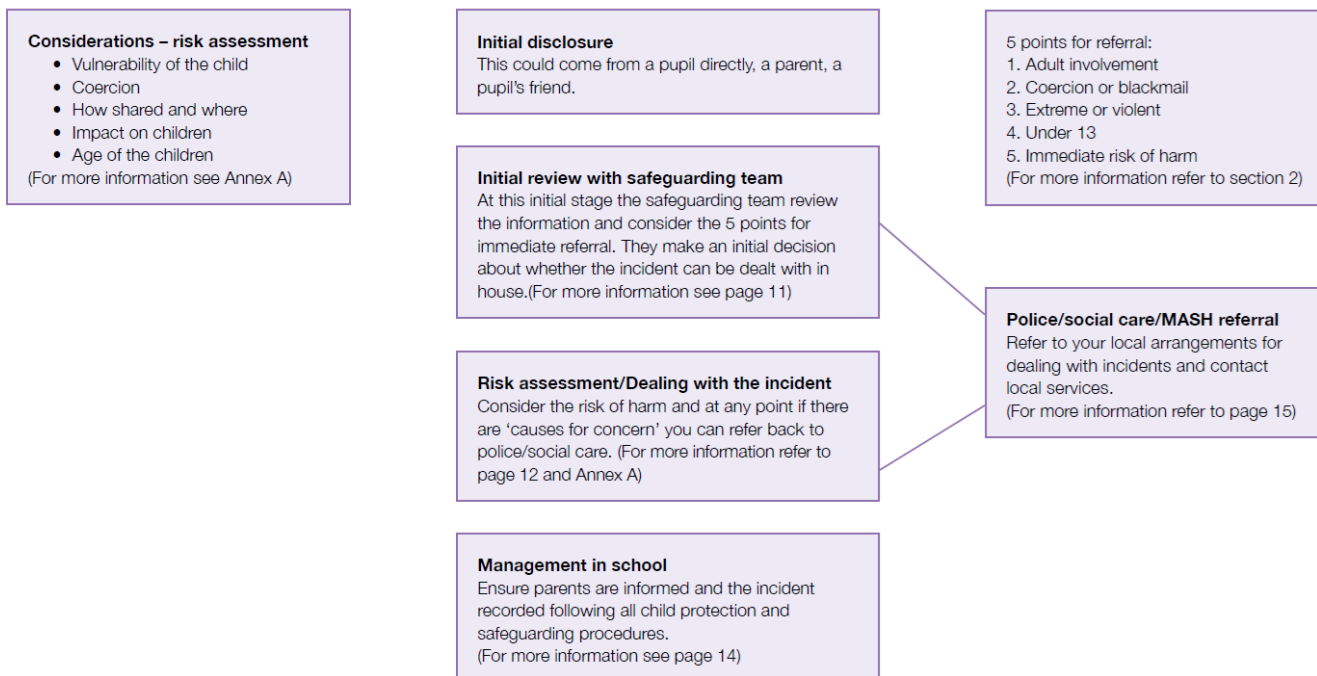
The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved.

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

The documents referenced above and materials to support teaching about sexting can be found at [sexting.lgfl.net](http://sexting.lgfl.net).

# Annex G

## Flowchart for responding to incidents





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

## **Bullying**

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying. Wanstead High School clearly outlines this in its Anti-bullying Policy.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at [bullying.lgfl.net](http://bullying.lgfl.net).

## **Sexual violence and harassment**

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

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

## **Misuse of school technology (devices, systems, networks or platforms)**

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

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

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

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

## **Social media incidents**

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

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

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Wanstead High School will request that the post be deleted and will expect this to be actioned promptly.

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

### **Data protection and data security**

GDPR information on the relationship between the school and LGfL can be found at [gdpr.lgfl.net](http://gdpr.lgfl.net); there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

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

All students, staff, governors, volunteers, contractors and parents are bound by the school’s data protection policy and agreements.

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

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with

appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data with external agencies. If this is not possible, the DPO and DSL should be informed in advance.

### **Appropriate filtering and monitoring**

Keeping Children Safe in Education obliges schools to “ensure appropriate filters and appropriate monitoring systems are in place to be able to block access to harmful or inappropriate materials”.

At this school, the internet connection is provided by LGfL. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools. You can read more about why this system is appropriate on the UK Safer Internet Centre’s appropriate filtering submission pages [here](#).

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

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

At Wanstead High School, we have decided that option a combination of all three is appropriate as this enhances our culture of vigilance.

### **Electronic communications**

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Staff Code of Conduct. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

#### **Email**

- Students at this school use the email facility within Google Classroom
- Staff at this school use the school’s Office 365 platform.

Both these systems are fully auditable and trackable. This is for the mutual protection and privacy of all staff, students and parents, as well as to support data protection.

General principles for email use are as follows:

- Email alongside the chat functionality of Google Classroom is the only means of electronic communication to be used between staff and students / staff and parents (in both directions). Use of a different platform must be approved in advance by the Data Protection officer / Headteacher. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO 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, Egress systems are available from LGfL.

- Internally, staff should use the school network, including when working from home when remote access is available via Terminal Services
- 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
- Students and 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 may be blocked and not arrive at their intended destination. If any staff or pupils know of anyone using the system for personal use, this must be reported to the Headteacher immediately.
- 

## **School Website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Ms S Axtell.

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at [safepolicies.lgfl.net](https://safepolicies.lgfl.net) to help schools to ensure that all requirements are met.

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with Ms N Roy. There are many open-access libraries of high-quality public-domain images that can be used. Students and staff at LGfL schools also have access to licences for music, sound effects, art collection images and other at [curriculum.lgfl.net](https://curriculum.lgfl.net).
- 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 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’](#).

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our DP policy here.

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

The following principles apply:

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

### **Digital images and video**

When a pupil/student joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

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

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

Any students shown in public facing materials are never identified with more than first name.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of students, and where these are stored. At Wanstead High School no member of staff will ever use their personal phone to capture photos or videos of students.

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

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

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.

Students are taught about how images can be manipulated in their online safety education.

Students 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.

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

## **Social Media**

### **Wanstead High School's social media presence**

Wanstead High School works on the principle that if we don't manage our social media reputation, someone else will. 'We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing.' Any concerns regarding a staff members conduct online must be reported to the Headteacher and DSL immediately.

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

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

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

Donna Cini is responsible for managing our Twitter accounts and checking our Wikipedia and Google reviews. S/he follows the guidance in the LGfL / Safer Internet Centre online-reputation management document [here](#).

### **Staff, students and parents' social media presence**

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and students will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect

everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

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

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

Many social media platforms have a minimum age of 13, but the school sometimes deals with issues arising on social media with students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that 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 students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The school has an official Twitter / Instagram account (managed by Donna Cini and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

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

Students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). If a pupil or parent/carer follows a public personal staff account, the request must be removed immediately and reported to the Headteacher and DSL.

\* 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 are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school or local authority, bringing the school into disrepute.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been 200 Prohibition Orders issued to teachers over the past four years related to the misuse of technology/social media.

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

### **Device usage**

Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

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

- **Students** are allowed to bring mobile phones in for emergency use only on the way to or home from school. During lessons, phones must remain turned off at all times, unless the teacher has given express permission as part of the lesson. Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to confiscation. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to students in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and data protection and data security section of this document. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents.** When at school events, please refer to the Digital images and video section of this document. [[parentfilming.lgfl.net](http://parentfilming.lgfl.net) may provide further useful guidance]. Parents are asked not to call students on their mobile phones during the school day; urgent messages can be passed via the school office.

### **Network / internet access on school devices**

- **Students** are not allowed networked file access via personal devices.



- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and Data protection and data security section of this document. Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices

### **Trips / events away from school**

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

### **Searching and Confiscation**

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher, DSL and staff authorised by them have a statutory power to search students' 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.

### **Delivering Live Lessons**

Live Lessons can be planned for in the event of any remote learning scenario.

Live Lessons should be delivered in the event of **Scenario 'B' - a teacher having to self-isolate, however is well, Scenario 'C' - a partial lockdown** for example where one or more-year groups are taught remotely or **Scenario 'D' - a full lock down**, if all students are learning from home.

Staff are expected to follow the following guidance as outlined in our Remote Learning Framework;

- Notify your CTL/line manager as to when and which groups you will be delivering Live Lessons to (agree a Live Lesson schedule to plan which lessons are best delivered Live/Loom or Google Classroom).
- CTLs/line managers will discuss and agree your Live Lessons timetable with you.
- Live Lessons should only be delivered during school timetabled hours.
- CTLs/line managers will keep a log of and keep a log of who's doing Live Lessons and when for their departments.
- Live Lessons are to be delivered via Google Meets, within the Google Classroom Suite.
- Decide if you plan to deliver your Live Lesson with audio only or both audio/video.

- Ideally the Live Lesson should take place on school premises.
- However, if teaching a Live Lesson from your home, prepare to teach your live lesson set up against a neutral background where nothing personal or inappropriate can be seen or heard.
- Avoid streaming a live lesson in a bedroom, if you can (if that's not possible, use a neutral background).
- Dress-code must be as per the school's code of conduct, as you would for work.
- On your PC/Laptop double check that any other tabs you may have open in your browser would be appropriate for a child to see, especially if you plan on sharing your screen.
- Always use professional language in your Live Lesson delivery.
- Be sensitive to the needs of individual students, including SEND and EAL, and also and children who may be sensitive to certain topics or issues that may arise during the Live Lesson content.

### **Recording a video or Loom lesson**

- If recording a video or Loom lesson from your home, prepare to record against a neutral background where nothing personal or inappropriate can be seen or heard.
- Avoid recording in a bedroom, if you can (if that's not possible, simply use a neutral background).
- Dress-code must be as per the school's code of conduct, as you would for work.
- On your PC/Laptop double check that any other tabs you may have open in your browser would be appropriate for a child to see, especially if you plan on sharing your screen.
- Always use professional language in your lesson delivery.
- Store the loom lesson or recording on a secure school system
- The Recording should only contain what is adequate, relevant and limited to the subject-matter being taught and should not contain unnecessary personal information or controversial opinions or comments that may cause offence. This will ensure the data held by the school remains professional in nature.
- Loom Access Settings. You have two options available. Whilst logged into your Loom Account, click on a specific Loom Video. To the right of the screen you will see 'Access Control'. Select 'Anyone on the web can find and access the video. No login required'. Alternatively, switch this Access off by sliding the green tab to the left and instead, invite students by email to limit who is able to watch your video.

Only use your Loom account that you have set up for work only, not personal use. For example, for Loom Lessons use account [Yourfirstinitial.surname@elearning.wansteadhigh.co.uk](mailto:Yourfirstinitial.surname@elearning.wansteadhigh.co.uk)