Online Safety Policy

Reviewed By: Computing Leader Date: September 2021

Ratified By: Avril Stockley Date: September 2021

Date of next review: September 2022

Introduction

Key people / dates

William Hogarth School 	Designated Safeguarding Lead	Avril Stockley
	Deputy Designated Safeguarding Lead	Katie Rees
	Nominated Safeguarding Governor	David Brennan
	Chair of Governors	Debra Kane
	Computing Lead	David Hannah

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' 2019 (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 sits alongside the school's child protection and safeguarding policy. 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 is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, school staff, governors, pupils and parents should be involved in writing and reviewing the policy, making use of day-to-day experience on the ground. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies for different stakeholders help with this.

Who is in charge of online safety?

The designated safeguarding lead takes lead responsibility for safeguarding and child protection (including online safety).

What are the main online safety risks today?

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

Many of these new risks are mentioned in KCSIE 2019, e.g. fake news, upskirting and sticky design.

The LGfL DigiSafe 2018 pupil survey of 40,000 pupils 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.

How will this policy be communicated?

This policy must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website.
- Available on the internal staff network/drive.
- Part of school induction pack for new staff.
- Integral to safeguarding updates and training for all staff.
- Clearly reflected in the Acceptable Use Policies (AUPs).
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

Contents

Introduction 2
Key people / dates 2
What is this policy? 2
Who is it for; when is it reviewed? 2
Who is in charge of online safety? 2
What are the main online safety risks today? 3
How will this policy be communicated? 3
Contents 4
Overview 5
Aims 5
Roles and responsibilities 5
Governors 6
Headteacher and SLT 6
ICT Technician 6
All staff 7
Pupils 7
Parents/carers 8
Education and curriculum 8
Handling online-safety concerns and incidents 8
Online safety concerns 10
Misuse of school technology (devices, systems, networks or platforms) 11
Email 11
School website 12
Digital images and video 12
Social media 13
William Hogarth's SM presence 13
Staff, pupils' and parents' SM presence 13
Device usage 14
Personal devices 14
Searching and confiscation 14

Overview

The William Hogarth School subscribes to https://nationalonlinesafety.com/ and has achieved the certified school status for online safety. The four steps to achieve this status are as follows:

- Designated Safeguarding Leads will need to complete the new Level 3 Course in Online Safety.
- Teachers will need to complete the new Level 2 course in Online Safety.
- The school will roll out the hub to a minimum of 10 users.
- Engage parents and other users in resources, guides and webinars.

Aims

This policy aims to:

- Set out expectations for all William Hogarth 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.

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.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the governor responsible for Safeguarding. The role will include:

- Ensure an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders.
- Ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to.
- Hold the headteacher and staff accountable for online safety.

Headteacher and SLT

The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community. Any complaint about staff misuse must be referred to the headteacher. Responsibilities include:

- Ensure access to induction and training in online safety practices for all users.
- Ensure all staff receive regular, up to date training.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured.
- Work in partnership with the DfE and the Internet Service Provider to ensure systems to protect students are appropriate and managed correctly.
- Ensure the school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.

ICT Technician

The William Hogarth School has a partnership with ClickOnIt London who provides a technician to regularly visit the school to support maintenance of technology. The ICT technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply.

- That users may only access the networks and devices through a properly enforced password protection policy.
- That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.

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) is.
- 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 on CPOMs and on the online safety log.
- Sign and follow the staff acceptable use policy.
- Whenever overseeing the use of technology in school or setting as homework tasks, encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.
- Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem.
- 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.
- 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.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil acceptable use policy.
- 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.

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, pupils or other parents/carers.

Education and curriculum

The following subjects have the clearest online safety links:

- PSHE
- Relationships and sex education (RSE)
- Computing
- Citizenship

The computing curriculum is designed so that all classes (1-6) will learn about online safety in the Autumn term. However, learning should be revisited throughout the year when topics arise from children or events occur (such as safer internet day). Teachers will follow the resources on PiXL to offer children a broad and in depth understanding of online safety. This learning includes but is not limited to: using the internet, personal information, using emails, online games and apps, cyberbullying, online situations, digital footprints, online scams and online chatting.

At the beginning of the year each class will also complete an audit of online platforms used. Through this, teachers will be able to understand which children have their own online accounts or if they use someone else's account. Children will also have the opportunity to discuss any websites not covered. Teachers will inform pupil's on age restrictions on websites and the importance of parent monitoring online use.

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.

The incident should be placed onto CPOMs to inform the DSL and the computing lead. The purpose of the online safety log on CPOMs is to analyse where trends/patterns occur between groups of children, if any viral videos are being spread around the school or if new online platforms are being used. This monitoring will enable prompt and effective action to be taken.

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

Online safety concerns

The following safety concerns are also mentioned in the William Hogarth child protection and safeguarding policy:

Sexting

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. 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) 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, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

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

Cyberbullying

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.

Sexual violence and harassment

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

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

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

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

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

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

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.

Email

Staff at this school use the LGFL StaffMail system for all school emails.

The email 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:

- Parent contact through email should be used by the admin email account. Except for special circumstances such as during a school closure.
- Staff or pupil personal data should never be sent/shared/stored on email.

    - Internally, staff should use the school network, including when working from home when remote access is available.
- 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.

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 school website should contain all the information as determined by the DfE.

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.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

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.

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

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

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. At the William Hogarth School no member of staff will use their personal phone to capture photos or videos of pupils. If a member of staff uses a personal phone to capture photos or videos of pupils, these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Social media

William Hogarth's SM presence

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 (Mumsnet is a favourite).

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

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

Teaching staff members, including the headteacher and deputy headteacher are responsible for uploading onto our twitter account and should do so in accordance with the online safety policy.

Staff, pupils' and parents' SM presence

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

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

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

Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. 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/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).

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

- **Pupils** in Year 5 and 6 only are allowed to bring mobile phones in for emergency use but they must be stored in the office in a secured place. No wearable technology is allowed by pupils.
- **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.
- **Volunteers, contractors, governors** should leave their phones in their pockets and on silent.

Searching and confiscation

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