GLC All Different: All Equal
Together, Improving Upon Our Best

GLC Online Safety Policy

GLC Staff were consulted on this document on :	Autumn 2021
This Policy was ratified by the Board of Directors on :	Spring 2022
This Policy will be reviewed by the GLC Board on :	Spring 2024

GLC Mission Statement

The GLC’s mission is to develop active and thriving citizens within a diverse, truly fair and equal community.

This will be achieved through:

- High quality teaching that deliberately develops competencies of curiosity, creativity, communication and critical-thinking;
- An inspiring and meaningful curriculum;
- The development of productive relationships by instilling the values of compassion, resilience, responsibility and aspiration to prepare our young people for learning and life;
- A commitment to the wellbeing of our staff;
- A culture of professional generosity, collaboration, challenge and support throughout the GLC;
- The development of effective external partnerships for the benefit and wellbeing of our community.

Equalities Statement

The GLC’s commitment to equality is enshrined in our mission statement to develop ‘active and thriving citizens within a diverse, truly fair and equal community’.

We are a vibrant, innovative and successful organisation: we work hard to be the place of choice to work and to learn. Across the 5 academies of the GLC, we pledge that everyone enjoys an equality of opportunity. We work tirelessly to ensure that individual characteristics including age, ethnicity, socio-economic background, academic ability, disability, gender, religious beliefs, sexual orientation are not discriminated against in any way. We create inclusive environments characterised by mutual respect where difference is celebrated.

Table of Contents

GLC Online Safety policy

1. Introduction

Use of new technology needs to be something we are building into our strategies to reach out and connect with young people. However, with every new release or update comes a new risk or element to be aware of. Never before has it been so important for young people and for those of us who work with young people to be kept safe online, and in every other form of e-communication.

2. Rationale

- The GLC welcomes the development of new technologies for communicating and will use them wherever they are appropriate to enhance our work with young people;
- We recognise our responsibility to take all reasonable measures to ensure that the risks of harm to young people's welfare are minimised; and, where there are concerns about young people's welfare, to take appropriate actions to address those concerns;
- We recognise the need to protect staff and volunteers from inappropriate conduct from young people in their personal lives and from situations that may make them vulnerable to allegations of wrongful conduct;
- We acknowledge that working for the GLC requires appropriate conduct in public spaces outside or work and in our personal lives and that this includes electronic communication.
- This policy sets out the ways in which the Gateway Learning Community will:
  - Educate all members of the school community on their rights and responsibilities with the use of technology;
  - Build both an infrastructure and culture of online safety;
  - Work to empower the school community to use the Internet as an essential tool for life-long learning.

3. Definition

- Electronic communication includes using mobile phones, computers and other devices for email, text, instant messaging and social networking.

4. Compliance with Safeguarding Children Agenda

- The GLC will ensure that our staff and volunteers follow the requirements of all relevant legislation as the policies and procedures of the local Safeguarding Children Board;
- We will train our staff and volunteers to follow this policy and we will regularly monitor its implementation.

5. Policy Review

- The GLC online safety policy will be reviewed every two years and will be under continuous revision in response to significant new developments in the use of technologies, new threats to online safety or incidents that have taken place. Our Policy has been written by the GLC, building on a London Grid for Learning [LGfL] policy template; 'Keeping Children Safe in Education' 2021 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents]. This document should be read in conjunction with the GLC policies on behaviour, safeguarding, anti-bullying and data protection.

6. Scope of policy

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

- The GLC will manage online safety as described within this policy and associated behaviour and anti-bullying policies, and will inform parents and carers of known incidents of inappropriate online safety behaviour that take place in and out of school.

7. Schedule for Development, Monitoring and Review

The impact of the policy will be monitored by each GLC Head of School by looking at:

- The academy log of reported incidents;
- Surveys or questionnaires of learners, staff, parents and carers;
- Other documents and resources.

8. Roles and responsibilities

The GLC IT Manager and Technical Staff will:

- Ensure that the GLC's IT infrastructure/network is as safe and secure as possible, and will an audit to annually review online safety with the school's technical support.
- Support the HT and DSL team as they review protections for pupils in remote-learning procedures, rules and safeguards
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls

Each GLC Head of School is responsible for ensuring the safety [including online safety] of all members of the academy community.

The Head will:

- Ensure that policies and procedures approved within this policy are implemented
- Ensure that suitable training is in place for all staff;
- Create a culture where staff and learners feel able to report incidents
- Ensure that there is a system in place for monitoring online safety
- Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil
- Inform the local authority about any serious online safety issues
- Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety

The designated Child Protection Coordinator for each GLC academy, will also act as the Online safety Leader and will have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying. The designated Online safety Lead will:

- Represent their academy at the GLC Inclusion Task Group [where Online safety will be discussed];
- Log, manage, and inform others of online safety incidents and how they have been resolved where this is appropriate;
- Lead the establishment and review of online safety policies and documents;
- Lead and monitor a progressive online safety curriculum for pupils;
- Ensure all staff are aware of the procedures outlined in policies relating to online safety;
- Provide and/or broker training and advice for staff;
- Attend updates and liaise with the LA online safety staff and technical staff;
- Meet with Senior Leadership Team and online safety Governor to regularly discuss incidents and development

The GLC Inclusion Task Group will assume the responsibility for monitoring the implementation of this policy across the trust.

The GLC Board will:

- review the policy every two years or when significant changes are warranted due to new legislation of a change in circumstances.
- 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
- will nominate governor to oversee their academy's actions to support each pupil's Personal Development, Behaviour and Welfare: this will include staying safe online.

- Teaching and support staff will:
  - Participate in any training and awareness raising sessions;
  - Act in accordance with the GLC and online safety Policy;
  - Report any suspected misuse or concerns to the Online Safety Leader and check this has been recorded;
  - Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this)
  - Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
  - Provide appropriate Online safety learning opportunities as part of a progressive online safety curriculum;
  - 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.
  - Monitor ICT activity in lessons, extracurricular and extended school activities;
  - Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a critical incident [please see below for further guidance].

- The PSHE/RSHE lead in addition to the 'Teaching and support staff' section, will:
  - Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education (RSE) and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives."
  - This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
  - Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

- The Computing lead in addition to the 'Teaching and support staff section, will:
  - Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
  - Work closely with the RSHE lead to avoid overlap but ensure a complementary whole-school approach

- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

- Pupils will:
  - Participate in online safety activities, report concerns for themselves or others;
  - Understand that this online safety policy covers actions out of the GLC that are related to their membership of the GLC.
  - Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
  - Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
  - Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
  - Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
  - Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
  - To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
  - Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.

- Parents and carers will:
  - Support this policy by signing the GLC Home Academy Contract and pupil AUP [Appendix 1 and Appendix 2]
  - Discuss online safety issues with their child(ren) and monitor their home use of technology [including tablets, mobile phones and games devices] and the Internet;
  - Inform their GLC Head of School of any online safety issues that relate to the academy;
  - Maintain responsible standards when using social media to discuss GLC issues.
  - Promote positive online safety and model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
  - Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
  - Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changed where possible.

9. Education of pupils

- *Pupils should 'understand what constitutes unsafe situations and are highly aware of how to keep themselves and others safe in different situations including in relation to online safety'*
  School Inspection Handbook - Ofsted 2014

- The GLC will ensure a comprehensive planned online safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited [please see the GLC primary and secondary curriculum policies];

- All GLC academies will ensure:
  - Key online safety messages are reinforced through assemblies, Safer Internet Week [February], anti-bullying week [November] and throughout all lessons

- Pupils are taught to keep themselves safe online and to be responsible in their use of different technologies;
- Pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material;
- In lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- Pupils are taught to be critically aware of the content they access online and are guided to validate the accuracy and reliability of information;
    - pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
    - pupils are taught about current issues such as online gaming, extremism, vlogging and obsessive use of technology;
    - pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying'

10. Handling of 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 (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Sexual Harassment / Peer on Peer Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)
- 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 pupils when they come into school or during extended periods away from 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

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for sexting and upskirting; see section below).

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

10.1 Sexting – sharing nudes and semi nudes

- All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.
- There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.
- The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

10.2 Upskirting

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

10.3 Cyberbullying

- Cyberbullying [along with all other forms of bullying] of any member of the school community will not be tolerated. Full details are set out in the GLC's policy on anti-bullying and behaviour;
- The GLC academy will follow procedures in place to support anyone in the school community affected by cyberbullying.
- Pupils and staff are made aware of a range of ways of reporting concerns about cyberbullying e.g. telling a trusted adult, ChildLine Phone number 0800 1111.
- Pupils, staff and parents and carers will be encouraged to report any incidents of cyberbullying and advised to keep electronic evidence.
- All incidents of cyberbullying reported to the GLC academy will be recorded by that academy.
- The academy will follow standard procedures to investigate incidents or allegations of cyberbullying.
- The academy will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police.
- Pupils, staff and parents and carers will be required to work with the academy to support the approach to cyberbullying and the school's online safety ethos.

10.4 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.

10.5 Misuse of School Technology [devices, systems, networks or platforms]

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

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

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

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

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

10.6 Social Media Incidents

- See the social media section later in this document for rules and expectations of behaviour for children and adults in the GLC community. These are also governed by school Acceptable Use Policies.
- Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct/handbook (for staff).
- Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, the GLC will request that the post be deleted and will expect this to be actioned promptly.
- Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

11. Technical Infrastructure

The GLC's IT manager will ensure:

- The GLC IT systems are managed in ways that ensure that the school meets online safety technical requirements;
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the GLC systems and data with regard to:
  - The downloading of executable files by users;
  - The extent of personal use that users [staff/pupils/community users] and their family members are allowed on laptops and other portable devices used out of school;
  - The installing programs on GLC devices unless permission is given by the technical support provider or Computing/ICT coordinator;
  - The use of removable media [e.g. memory sticks] by users on GLC devices.
  - The installation of up to date virus software;

- access to the GLC network and Internet will be controlled with regard to:
    - users having clearly defined access rights to GLC IT systems;
    - users [apart from possibly Foundation Stage pupils] being provided with a username and password;
    - staff users being made aware that they are responsible for the security of their username and password; they must not allow other users to access the systems using their log on details;
    - the 'master/administrator' passwords are available to the GLC Business Manager and CEO and kept in the Gateway Academy finance safe;
    - an agreed process being in place for the provision of temporary access of 'guests' [e.g. trainee or supply teachers, visitors] onto the GLC system. All 'guests' must sign be made aware of this online safety policy

12. Data Protection

Please see the GLC's Data Protection Policy.

13. Use of digital and video images

Photographs and video taken within the GLC are used to support learning experiences across the curriculum, to share learning with parents and carers and to provide information about the school on the website. The GLC will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites;
- Allow staff to take images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those image;
- Make sure that images or videos that include pupils will be selected carefully with their knowledge;
- seek permission from parents or carers before images or videos of pupils are electronically published;
- Encourage pupils to seek permission from other pupils to take, use, share, publish or distribute images of them without their permission;
- All parties must recognise that any published image could be reused and repurposed;
- Make sure that pupils' full names will not be used anywhere on the school website, particularly in association with photographs, unless permission has been given in advance;
- Not publish pupils' work without their permission and the permission of their parents;
- Keep the written consent where pupils' images are used for publicity purposes, until the image is no longer in use;
- Publish a policy regarding the use of photographic images of children which outlines policies and procedures including disposal and deletion.

14. Communication

A wide range of communications technologies have the potential to enhance learning.
The GLC will:

14.1 With respect to email

- Ensure that the GLC uses a secure business email system for communication;
- Ensure that personal information is not sent via unsecure email;
- Ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content;

- Make users aware that email communications will be monitored by the GLC;
- Inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature;
- Use email at KS1 through a group or class activity with an adult sending and opening emails**;**
- Provide pupils at Key Stage 2 with a monitored individual educational school email addresses.

14.2 With respect to mobile phones

- **Pupils** are allowed to bring mobile phones in for emergency use only in Primary and must be handed to the class teacher at the start of the day switched off. At Secondary, pupils may use mobile phones during lunch break, but not when moving around the school buildings. 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 following the GLC Behaviour Policy and the withdrawal of mobile privileges. Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- Under no circumstances are pupils in primary are allowed to wear smart devices to school that have the ability to call or record or display sound or visual media. In secondary, wearable smart devices must be used in line with the GLC Mobile Phone Policy.
- **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 on page and Data protection and data security section on page. 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** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

15. Assessment of risk

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the GLC will examine and adjust the online safety Policy. Part of this consideration will include a risk assessment,

- looking at the educational benefit of the technology;
- considering whether the technology has access to inappropriate material;

However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The Gateway Learning Community cannot accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

16. The police will be informed where users:

visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images

- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

17. Sanctions and Disciplinary proceedings

Sanctions and disciplinary procedures may be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to [unless this is part of an investigation]:

- Child Sexual abuse images;
- Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003;
- Pornography, adult or mature content;
- Promotion of any kind of discrimination, racial or religious hatred;
- Personal gambling or betting;
  Personal use of auction sites;
- Any site engaging in or encouraging illegal activity;
- Threatening behaviour, including promotion of physical violence or mental harm;
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- Using school systems to run a private business;
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school;
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- Revealing or publicising confidential or proprietary information [e.g. financial or personal information, databases, computer or network access codes and passwords];
- Creating or propagating computer viruses or other harmful files;
- Carrying out sustained or instantaneous high volume network traffic [downloading or uploading files] that causes network congestion and hinders others in their use of the Internet.

18. The Gateway Learning Community Social Media Presence

The GLC works on the principle that if we don’t manage our social media reputation, someone else will.

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

18.1 With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- Enable online learning opportunities to make use of age-appropriate educationally focussed sites that will be moderated by the GLC;
- Control access to social-media and social-networking sites in GLC;

- Provide the online safety protocol [see Addendum below] for staff to use GLC approved social media and online learning platforms securely;
- Through the IT team, additional requested platforms will be assessed for safety, suitability and GDPR;
- Have a process supported and monitored by the GLC's IT Manager to enable teachers who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences;
- Provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given;
- Make sure that staff official blogs will be password protected and run from the GLC website with approval from the GLC Head of School;
- Ensure that any digital communication between staff and pupils or parents and carers is always professional in tone and content;
- Clarify with staff that the sharing with pupils and use of personal email, social media and personal publishing is prohibited;
- Authorise and supervise any social media accounts used for educational purposes;
- Discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with Teaching Standards 2012;
- Advise all members of the school community not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory;
- Register concerns [e.g. recording in online safety log] regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites [in or out of school] and raise with their parents and carers, particularly when concerning pupils' underage use of sites;
- Inform the staff that in the case of a **critical incident** they should not make any comment on social media without the permission of the senior management team

18.2 Staff, pupils' and parents' Social Media Presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.
This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we 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 (note that WhatsApp is 16+), but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures 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 (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

The schools have official Facebook / Twitter / Instagram accounts managed by a Senior Leader and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Class Dojo and is the official electronic communication channel between parents and the school, and between staff and pupils within the Primay Schools.

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

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

> * Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Headteacher/Principal, and should be declared upon entry of the pupil or staff member to the school).
> ** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

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

Appendix 1

My name is ________________________________

To stay **SAFE online and on my devices**,

1. I only **USE** devices or apps, sites or games if a trusted adult says so □
2. I **ASK** for help if I'm stuck or not sure □
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused □
4. I look out for my **FRIENDS** and tell someone if they need help □
5. I **KNOW** people online aren't always who they say they are □
6. Anything I do online can be shared and might stay online **FOREVER** □
7. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to □
8. I don't change **CLOTHES** or get undressed in front of a camera □
9. I always check before **SHARING** personal information □
10. I am **KIND** and polite to everyone □

My trusted adults are:

_________________________at school
_________________________ at home

For parents/carers

To find out more about online safety, you can read The Gateway Learning Community's full Online Safety Policy [http://www.theglc.org.uk/170/key-information] for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).
You can find support, online safety advice and lots of tips for safe settings and controls for parents at parentsafe.lgfl.net

Appendix 2

These statements can keep me and others safe & happy at school and home

1. *I learn online* – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. *I learn even when I can't go to school because of coronavirus* – I don't behave differently when I'm learning at home, so I don't say or do things I wouldn't do in the classroom and nor do teachers or tutors. If I get asked or told to do anything that I would find strange in school, I will tell another teacher.
3. *I ask permission* – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
4. *I am creative online* – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things.
5. *I am a friend online* – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
6. *I am a secure online learner* – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
7. *I am careful what I click on* – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
8. *I ask for help if I am scared or worried* – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
9. *I know it's not my fault if I see or someone sends me something bad* – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
10. *I know new online friends might not be who they say they are* – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. *I check with a parent/carer before I meet an online friend* the first time; I never go alone.
12. *I don't do live videos (livestreams) on my own* – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. *I keep my body to myself online* – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell

me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. *I say no online if I need to* – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. *I tell my parents/carers what I do online* – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. *I am private online* – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
17. *I am careful what I share and protect my online reputation* – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
18. *I am not a bully* – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
19. *I am part of a community* – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
20. *I am a researcher online* – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

Outside school, my trusted adults are____________________________________

I know I can also get in touch with Childline

Signed: ________________________ **Date:** ____________________

For parents/carers

To find out more about online safety, you can read The Gateway Learning Community's full Online Safety Policy [http://www.theglc.org.uk/170/key-information] for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).
You can find support, online safety advice and lots of tips for safe settings and controls for parents at parentsafe.lgfl.net
~~~~~~~~~~~~~~~~~~~~~~