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

GLC Online Safety Policy

This Policy was ratified by the Board of Directors on :	Autumn 2024
This Policy will be reviewed by the GLC Board on :	Autumn 2026

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

1. Introduction..... 3
2. Rationale/aims……..3
3. Definition.....3
4. Compliance with Safeguarding Children Agenda.....4
5. Policy Review.....4
6. Scope of policy.....4
7. Schedule for Development, Monitoring and Review..... 4
8. Roles and responsibilities.....4
9. Education of pupils and parents/carers..... 8
9.1 Training of staff……9
9.2 Handling of Online Safety Concerns and Incidents..... 9
10. Sexting – sharing nudes and semi nudes.....10
10.1 Upskirting.....10
10.2 Cyberbullying..... 10
10.3 Sexual Violence and Harassment..... 11
10.4 Misuse of School Technology [devices, systems, networks or platforms]..... 11
10.5 Examining electronic devices……11
10.6 Artificial intelligence [AI]…… 12
10.7 Social Media Incidents.....12
10.8 Technical Infrastructure……..…13
11. Data Protection..... 13
12. Use of digital and video images.....13
13. Communication..... 14
13.1 With respect to email..... 14
13.2 With respect to mobile phones and smart devices.....14
14. Assessment of risk.....15
15. The police will be informed where users:.....15
16. Sanctions and Disciplinary proceedings.....16
17. The Gateway Learning Community Social Media Presence.....17
18. Staff using work devices outside of school……17
18.1 With respect to social media e.g. YouTube, Facebook, X, blogging and personal publishing.....17
18.2 Staff, pupils' and parents' Social Media Presence..... 18

GLC Online Safety policy

1. **Introduction**
   - Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks;
   - We want to equip our pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world.
   - This policy brings together information that will help deliver online safety content within our curriculum and embed this within our wider whole school approach.
2. **Rationale/Aims**
   - 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;
   - We have robust processes in place to ensure the online safety of pupils/students, staff, volunteers, governors and directors;
   - As a trust, we identify and support groups of pupils/students that are potentially at greater risk of harm online than others;
   - Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in its use of technology, including mobile and smart technology [which we refer to as 'mobile phones'];
   - Establish clear mechanisms to identify, intervene and escalate incidents as identified in key policies
   - We are also fully aware of the need to take action to prevent child on child abuse which can happen in many forms [see paragraph 33 of KCSIE]. These may fall under new categories of criminal offences [part 10 of Online safety act 2023].

   The 4 key categories of risk:

   Our approach to online safety is based on addressing the following categories of risk:
   - Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
   - Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
   - Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images [e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography], sharing other explicit images and online bullying; and
   - Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

3. **Definition of electronic communication**
   - Electronic communication includes using mobile phones, computers and other devices for email, text, instant messaging, Artificial Intelligence based applications and social networking.

4. Compliance with the Safeguarding Children Agenda

Our policy has been written by the GLC, building on a London Grid for Learning [LGfL] policy template; 'Keeping Children Safe in Education' 2024 [KCSIE] 'Teaching Online Safety in Schools' January 2023 update, statutory PSHE/ RSHE guidance [last update September 2021] and other statutory documents]. This document should be read in conjunction with the GLC policies on behaviour, safeguarding, anti-bullying and data protection.

- We will train our staff and volunteers to follow this policy and we will regularly monitor its implementation.
- We will ensure a biannual online safety audit is conducted using the LGFL audit.

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.

6. Scope of policy

- This policy applies to all members of the GLC community [including teaching and support staff, supply teachers and tutors, governors, directors, volunteers, contractors, pupils/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 academy 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 academy.

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 [staff, governors and directors, pupils] of reported incidents;
- Surveys or questionnaires of learners, staff, parents and carers;
- Other documents and resources;
- The results will be shared with the board of directors on a half termly basis.

8. Roles and responsibilities

The GLC IT Director and Technical Staff will:

- Ensure that the GLC's IT infrastructure/network is as safe and secure as possible, and will conduct an audit to annually review online safety with the academy's technical support;
- Support the HT and DSL team as they review protections for pupils/students in remote-learning procedures, rules and safeguards;
- Keep up to date with the academy'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 and monitoring of 'appropriate filtering and monitoring' as decided by the DSL and in partnership with the senior leadership team;
- Ensure monitoring is daily during term time and weekly during holidays and referred to DSLs to take action as appropriate;
- Manage the academy 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 of School 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 systems for monitoring online safety are rigorous and robust;
- Follow correct procedure in the event of any online safety allegation being made against a member of staff, governor/director, pupil or parent;
- Inform the local authority/LSCP about any serious online safety issue;
- Ensure governors and directors are regularly updated on the nature and effectiveness of the academy's arrangements for online safety.

The Designated Safeguarding Lead 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 implementation and review of online safety policies and documents;
- Lead, monitor and evaluate 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 or director to regularly discuss incidents and development;
- Be responsible for understanding the filtering and monitoring systems that are in place.

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

- Review and monitor the policy twice during the academic year
- Ensure key/new information is shared back in each academy
- Discuss the common trends and key data to share back in each academy
- Feedback with case studies in order to share good practice

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;
- Nominate a governor or director to oversee their academy's actions to support each pupil's Personal Development, Behaviour and Welfare: this will include staying safe online.
- The board must ensure the academy has appropriate filtering and monitoring systems in place on academy devices and academy networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the academy in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

The Local Governing Body:

- The governing body has overall responsibility for monitoring this policy and holding the Head of School/DSL to account for its implementation;
- The governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring;
- The governing body will also make sure all staff receive regular online safety updates [via email, e-bulletins and staff meetings/briefings], as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children;
- The governing body will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead [DSL];
- The governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils/students with special educational needs and/or disabilities [SEND]. This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

Teaching, support staff, tutors and external providers will:

- Participate in any necessary training and awareness raising sessions;
- Act in accordance with the GLC and online safety policy;
- Report any suspected misuse or concerns to the DSL and check this has been recorded;
- Take a zero-tolerance approach to online bullying and 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 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 academy hours and site, and on social media, in all aspects upholding the reputation of the academy and of the professional reputation of all staff. More guidance on this point can be found here: https://lgfl.net/sites/default/files/LgflNet/downloads/online-safety/LGfL-OS-Advice-Online-Reputation-Managment-for-Schools.pdf;
- Not use personal logins/systems to communicate with or arrange meetings with students or parents. If staff are contacted they must report it to the DSL;
- Monitor ICT activity in lessons, extracurricular, extended academy activities and homework;
- 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 Curriculum/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/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 pupils/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 Computing subject leader to avoid overlap but ensure a complementary whole-academy approach, and with all other lead staff to embed the same whole-academy 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-cacademy 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 each academy to ensure a common and consistent approach, in line with acceptable-use agreements.

Pupils/students 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 [secondary] and adhere to the student/pupil acceptable use policy and review this annually;
- Treat home learning during any isolation/quarantine or bubble/academy lockdown in the same way as regular learning in academy and behave as if a teacher or parent were watching the screen;
- Be taught not to use personal logins/systems to communicate with or arrange meetings with academy staff or tutors;
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of academy 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 academy, 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 academy and realise that the academy's acceptable use policies cover actions out of academy, including on social media;
- Remember the rules on the misuse of academy technology – devices and logins used at home should be used just like if they were in full view of a teacher/parent.

Parents and carers will:

- Support this policy by signing the GLC Home Academy Contract and AUP with their child[ren] and monitor their home use of technology [including tablets, mobile phones and games devices] and the Internet;
- Inform their GLC DSL/ 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 academy staff, volunteers, governors/directors, contractors, pupils or other parents/carers;
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/academy 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.

Educating parents/carers about online safety

- The academy will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website/newsletters/communication platform. This policy will also be shared with parents/carers;
- Online safety will also be covered during parents information workshops during Internet Safety Week and at key transition points.

The academy will let parents/carers know:

- What systems the academy uses to filter and monitor online use;
- What their children are being asked to do online, including the sites they will be asked to access and who from the academy [if anyone] their child will be interacting with online;
- If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of School and/or the DSL;
- Concerns or queries about this policy can be raised with any member of staff or the Head of School.

9. Education of pupils/students and measures to prevent cyber-bullying

- 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/students will be taught about online safety as part of the curriculum.

The text below is taken from the National Curriculum computing programmes of study:

At primary pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private;
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact.

At secondary, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- Recognise inappropriate content, contact and conduct, and know how to report concerns;
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- How to report a range of concerns.

9.1 Training of staff

- All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation;
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as regular and relevant updates [for example through emails, e-bulletins and staff meetings].;
- By way of this training, all staff will be made aware that:
- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- Children can abuse their peers online through:
- Abusive, threatening, harassing and misogynistic messages;
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
- Sharing of abusive images and pornography, to those who don't want to receive such content;
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element;
- Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse;
- Develop the ability to ensure pupils/students can recognise dangers and risks in online activity and can weigh up the risks;
- Develop the ability to influence pupils/students to make the healthiest long-term choices and keep them safe from harm in the short term.
- The DSL [and deputy/deputies] will undertake level 3 child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually;
- Governors and directors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training;
- Volunteers will receive appropriate training and updates;
- More information about safeguarding training is set out in our child protection and safeguarding policy.

9.2 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].

Academy 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 academy sanctions];
- Acceptable Use Policies;
- Prevent Risk Assessment / Policy;
- Staff Code of Conduct and Whistleblowing Policy;
- Data Protection Policy, agreements and other documentation [e.g. privacy statement and consent forms for data sharing, image use etc].

The GLC 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/students when they come into the academy or during extended periods away from school. All members of the academy are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the academy'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 Head of School, unless the concern is about the Head of School 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 academy 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/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; see section below].

The academy 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. Sexting – sharing nudes and semi nudes

- All academies [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. Academies are also aware that pupils/students do sometimes share nudes consensually but should still be reported as within the one page overview [see point below];
- 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 academy 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.

10.1 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.

10.2 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/students 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/students, 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 academy 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.

10.3 Sexual Violence and Harassment

- DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education. Staff will be aware of this guidance which covers the immediate response to a report and confidentiality which is highly relevant for all staff;
- 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.

10.4 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.
- Where pupils/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.
- It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils/students 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.

10.5 Examining electronic devices

- The Head of School, or any member of staff authorised to do so by the Head of School [as set out in your behaviour policy – adapt to e.g. specify which staff are authorised], can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
    - Poses a risk to staff or pupils/students; and/or
    - Is identified in the school rules as a banned item for which a search can be carried out; and/or
    - Is evidence in relation to an offence.
    - Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
        - Make an assessment of how urgent the search is, and consider the risk to other pupils/students and staff. If the search is not urgent, they will seek advice from [the Head of School / DSL / appropriate staff member];
        - Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
        - Seek the pupil's co-operation.
- The safeguarding team in liaison with SLT, may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
    - Cause harm; and/or
    - Undermine the safe environment of the school or disrupt teaching; and/or
    - Commit an offence.
- If inappropriate material is found on the device, it is up to [the staff member in conjunction with the DSL / Head of School / other member of the senior leadership team] to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
    - They reasonably suspect that its continued existence is likely to cause harm to any person; and/or
    - The pupil and/or the parent/carer refuses to delete the material themselves.
- If a staff member **suspects** a device **may** contain an indecent image of a child [also known as a nude or semi-nude image], they will:
    - **Not** view the image ;

        - Confiscate the device and report the incident to the DSL [or equivalent] immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety [UKCIS] guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Any searching of pupils/students will be carried out in line with:
    - The DfE's latest guidance on searching, screening and confiscation;
    - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
    - Our behaviour and relationships policy.
- Any complaints about searching for or deleting inappropriate images or files on pupils/students' electronic devices will be dealt with through the school complaints procedure.

10.6 Artificial Intelligence [AI]

- Generative artificial intelligence [AI] tools are now widespread and easy to access. Staff, pupils/ students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.
- The GLC recognises that AI has many uses to help pupils/students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.
- The GLC will treat any use of AI to bully pupils/students in line with our [anti-bullying/behaviour] policy.

10.7 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/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, 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.

10.8 Technical Infrastructure

The GLC's IT Director 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/students/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;

- sers [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.

11 Data Protection

Please see the GLC's Data Protection Policy.

12 Use of digital and video images

Photographs and videos 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/students 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/students will be selected carefully with their knowledge;
- Seek permission from parents or carers before images or videos of pupils/students are electronically published;
- Encourage pupils/students to seek permission from other pupils/students 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/students' 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/students' work without their permission and the permission of their parents;
- Keep the written consent where pupils/students' 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.

13 Communication

A wide range of communications technologies have the potential to enhance learning.

The GLC will:

13.1 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/students 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/students at Key Stage 2,3 and 4 with a monitored individual educational school email addresses.

13.2 Acceptable use of internet in school

- All pupils/students, parents/carers, staff, volunteers and governors and directors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet [appendices 1 to 3]. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant;
- Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role;
- We will monitor the websites visited by pupils/students, staff, volunteers, governors, directors and visitors [where relevant] to ensure they comply with the above and restrict access through filtering systems where appropriate;
- Every Pupil device within the GLC be that on premises or a 1-2-1 device has all web traffic monitored / filtered by a product called "Smoothwall" this is a market leader in filtering solutions for schools & colleges in Europe;
- As part of the core IT teams remit each working day the previous days logs are checked for any violations and as such are reported [depending on the severity] to either the Class Teacher as guidance for the pupil to the other end of the scale on serious situations to the schools DSL.

13.3 With respect to mobile phones and smart technology

- Pupils [Y5/6]/students 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/students are not allowed to use mobile phones/electrical devices anywhere in the academy. The academy is "Mobile Free" and student mobile phones should not be used, seen or heard anywhere on the academy premises. Please see The GLC Behaviour Policy (Secondary). 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/students in emergencies;
- Under no circumstances are pupils in primary settings 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. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call they should liaise with their line manager. See the GLC Staff Code of Conduct;
- Only **GLC devices** should be used in the academy to take notes and photos. However, staff are permitted to access their email and google drive on personal devices but must follow the usual safety rules.
- **Volunteers, contractors, governors and directors** 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 Head of School should be sought [the Head of School 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 in the building. 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. Parents are asked not to call pupils/students on their mobile phones during the school day; urgent messages can be passed via the school office.

14 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 2022 and breaches will be reported to Police.

15 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.

16 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.
- Sanctions and disciplinary procedures may also be taken where users are in breach of the GLC Acceptable use of Technology Code of Conduct or Staff Code of Conduct.

17 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 Staff using work devices outside of school

- All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
  - Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters [e.g. asterisk or currency symbol];
  - Ensuring any hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
  - Making sure the device locks if left inactive for a period of time;
  - Not sharing the device among family or friends;
  - Keeping operating systems up to date by always installing the latest updates.
- Staff members must not use the device in any way that would violate the school's terms of acceptable use.
- Work devices must be used solely for work activities.
- If staff have any concerns over the security of their device, they must seek advice from the ICT Director.

18.1 With respect to social media e.g. YouTube, Facebook, X, 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 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 Director 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;
- Ensure that any digital communication between staff and pupils/students or parents and carers is always professional in tone and content;
- Clarify with staff that the sharing with pupils/students and use of personal email, social media and personal publishing is prohibited;
- Authorise and monitor 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 2021 ;
- 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/students' 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/students' 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 leadership team.

18.2 Staff, pupils/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 pupils/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, they should contact their academy 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 will cause upset to staff, pupils/students and parents, also undermining staff morale, the reputation of the school, bringing it into disrepute. The school will request any posts which contain inaccurate information to be removed or take legal action if required.

Many social media platforms have a minimum age of 13. We expect parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

GLC academies have official Facebook / X / Instagram accounts managed by the marketing and communications lead or members of staff and will respond to general enquiries about the school/ GLC, but asks parents/carers not to use these channels to communicate about their children.

Class Dojo is the official electronic communication channel between parents and the school, and between staff and parents within the Primary Schools. Edulink is the official electronic communication channel between parents and the school, and between staff and students within the Gateway Academy.

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

Pupils/students are discouraged from 'following' staff, governor, director, 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 Head of School, and should be declared/ self referred 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 Head of School [if by a staff member].

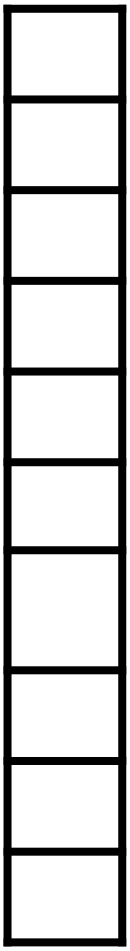
Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and 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*** – 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
~~~~~~~~~~~~~~~~~~~~

Acceptable Use of Technology Code of Conduct

Introduction

ICT in its many forms – internet, email, mobile devices etc. – are now part of our daily lives. It is our duty to ensure that they are used safely and responsibly. All staff working in the Gateway Learning Community Academies are aware of the following responsibilities:

• All Staff, Governors and visitors understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets;

• All staff, Governors and visitors understand that it is a disciplinary offence to use the school ICT equipment for any purpose not permitted by its owner;

• No staff, Governors or visitors will disclose any passwords provided to them by the school;

No staff, Governors or visitors will allow another person to use their network access credentials – regardless of the reason;

• All staff, Governors and visitors understand that they are responsible for all activity carried out under their username;

• Staff, Governors and visitors will not install any hardware or software on any school owned device without the GLC ICT Systems Director's express permission;

• All staff, Governors and visitors understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices. If an E-safety incident should occur, staff will report it to the Senior or Deputy Designated Professional for Child Protection as soon as possible;

• All staff, Governors and visitors will only use the school's email / internet / intranet etc. and any related technologies for uses permitted by the Head of School or Governing Body. If anyone is unsure about an intended use, they should speak to the GLC ICT Systems Director beforehand;

• All staff, Governors and visitors will ensure that data is kept secure and is used appropriately as authorised by the Head of School or Governing Body. No passwords should be divulged and memory sticks should also be encrypted;

• Personal devices must only be used in the context of school business with the explicit permission of the Head of School. Personal mobile phones or digital cameras must NEVER be used for taking any photographs related to school business. Each class has a digital camera specifically for this purpose. These school cameras must NEVER be used for personal use;

• All staff, Governors and visitors using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory;

• All staff, Governors and visitors will only use the approved email system for school business;

• Images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. At the start of each year, our parents are asked to sign if they agree to their children's images being used in our brochure or in the local press. If a parent does not agree to this, we ensure that their child's photograph is not used. Filming and photography by parents and the wider community at school events, such as sports days and school productions, are not allowed. When possible, a professional

photographer will come to school to take photographs of children, for example in their play costumes. These will then be made available to parents;

- All staff, Governors and visitors will make every effort to comply with copyright and intellectual property rights;

- All staff, Governors and visitors will report any incidents of concern regarding staff use of technology and/or children's safety to the Head of School or the Deputy Designated Professional in line with our school's Safeguarding Policy.

I acknowledge that I have received a copy of the Acceptable Use Code of Conduct.

Full Name: …… Signature: ……...

Date: …….. Position: …….

The Gateway Academy Laptop Guidance & Acceptable Use Contract

Laptop Use Contract

The purpose of this contract is to:

Guard against:- Theft of the laptop, Theft of the information stored on the laptop, Damage to the Laptop, Promote Appropriate & Acceptable use of the laptop.

This contract applies to all laptop computers owned by the school and is allocated to a particular member of staff for their use as an educational tool.

1. General
   1.1 All Laptops issued to members of staff on a long-term loan remain the property of the school.
   1.2 Staff should always bring their laptop into School. This allows for software updates, etc to be performed.

2. Password Protection
   2.1. To guard against unauthorised usage of the laptop a power on/start-up password must be enabled. This will be done by ICT Systems.

3. Data Protection
   3.1 Under no circumstances should students be allowed to use Staff laptops.
   3.2 Laptops should only be used by the member of staff, not their family and friends.
   3.3 Any data stored on your laptop, is subject to Data Protection laws, and as such, should only be viewed by The Gateway Academy Staff.
   3.4 Any breach of the above may result in the laptop being withdrawn from your use.

4. Laptops & Theft
   4.1. The user should take appropriate measures to protect the laptop and all its peripherals. When unattended, the laptop should be stored in a secure locked location.
   4.2. Do not leave the laptop in a vehicle, even if parked in your driveway or garage.
   4.3. Do not leave the laptop in Staffrooms.
   4.4. Should your laptop be stolen and you have been negligent, you will be charged the full cost of replacement.

5. Privacy & Monitoring
   5.1 The Gateway Academy reserves the right(s) to:-
   View any/all of the contents of your laptop.
   View/access all of your transactions across the network.
   View your email.

   5.2 Illegal actions are covered by the following acts:
   The Data Protection Act (1988)
   The Computer Misuse Act (1990)
   The Copyright, Designs and Patents Act (1988)
   Public Interest Disclosure Act (1998)
   Obscene Publications Act (1959)
   Telecommunications Act (1984)
   Theft Act (1968)
   The Gateway Academy can and will take disciplinary actions against offenders.

   5.3 Logs of all email sent to and from College accounts are stored on the College systems

6. Carrying Laptops
   6.1. Laptops should always be within the protective bag supplied with the laptop when carried.
   6.2. The carrying case should not be overloaded as this can damage the laptop screens.
   6.3. Laptops should be turned off properly before placing it in the carry case.
   6.4. The power connector should always be unplugged when the laptop is in the protective bag.
   6.5. Failure to do any of the above could damage the laptop and in extreme cases be a fire hazard
   6.6. Should your laptop be damaged due to negligence for whatever reason you will be charged full replacement cost.

7. Screen Care
   7.1. The laptop screen can be damaged if subjected to rough treatment.
   7.2. Do not lean on the laptop.
   7.3. Do not place anything on the keyboard as forgetting objects on the keyboard and closing the lid may cause damage to the screen.
   7.4. Do not place anything on top of the laptop when it is closed. This may cause damage to the screen.

8. Software
   8.1. The software originally installed on the laptops by ICT Systems should remain on the laptop and be maintained in usable condition. This is important when it comes to Antivirus software.
   8.2. Members of staff are responsible for ensuring that only software that is licensed to their laptop is loaded onto their computers.
   8.3. Due to copyright laws, personal software should not be loaded onto the laptops.
   8.4. All members of staff should comply with all trademark and copyright laws and all licence agreements.

9. Technical Support
   9.1. Do not attempt to repair any faults. All faults must be reported to & repaired by the ICT Systems team.
   9.2. Software support is limited to the software installed by the ICT Systems team.
   9.3. It is the member of staff's responsibility to ensure that their work is not lost due to mechanical failure or accidental deletion.

10. Backup
   10.1 Your laptop will not automatically back up your email & documents to the Network, Manual backups can be run by clicking "Sync with Network" on your start menu – this is down to yourself to complete.

Home School Laptop Agreement

The Gateway Academy Home Laptop Usage Agreement

Guidance and Acceptable Use Contract

Following the progress that has been made during the COVID-19 lockdown, the GLC has been given permission by Directors to launch a laptop loan scheme to selected year groups as a research pilot to see how learning is accelerated. This policy sets out the conditions for the loan. It aims to guard against the theft or damage to the laptop; the protection of information and software stored on the laptop and to set out the appropriate and acceptable use of the laptop. This contract applies to all laptop computers owned by the GLC.

1. General

1.1 All laptops are issued to each student on a long-term loan but remain the property of the GLC.

1.2 Any data stored on the laptop, is subject to the General Data Protection Regulations [GDPR] and as such, should only be viewed by authorised persons;

1.3 Any breach of GDPR may result in the laptop being withdrawn from your use;

1.4 The GLC can cancel this contract and take back the laptop at any time.

1.5 The Laptop will need to be returned to the GLC school either at the end of year 11, or if the student leaves the GLC school.

2. Laptop Care. Students, supported by the parents will:

2.1. Bring the laptop to school fully charged every day;

2.2. Carry the laptop to and around school in a suitable bag ensuring the charging cable has been removed.;

2.3. Treat the laptop with care as the screen can be damaged if subjected to rough treatment;

2.4. Not lean on, or overextend the laptop screen;

2.5. Not place anything on the keyboard [as objects on the keyboard will cause damage to the screen when the lid is closed];

2.6. Not place anything on top of the laptop when it is closed [as this may cause damage to the screen];

2.7. Not decorate or customise the computer and not allow it to be subject to graffiti.

2.8. Ensure that the laptop is only used on a hard surface allowing ventilation and removing the risk of overheating.

3. Theft and Damage

3.1. The user should take appropriate measures to protect the laptop and all its peripherals. When unattended, the laptop should be stored in a secure location.

3.2. The laptop must not be left in a vehicle, even if parked in a driveway or garage.

3.3. Should the laptop be stolen and you have been negligent, you will be charged the full cost of replacement.

3.4. If the laptop is stolen outside school, the police must be informed and a crime reference number obtained before informing the school;

3.5. Should your laptop be damaged, you may be liable to be charged for the repair or replacement cost.

4. Software

4.1. The software originally installed on the laptop by the GLC should remain on the laptop and be maintained in usable condition. This is important when it comes to antivirus software;

4.2. Students are responsible for ensuring that only software that is licensed to their laptop is loaded onto their computer;

4.3. Due to copyright laws, personal software should must not be loaded onto the laptops;

4.4. All students must comply with all trademark and copyright laws and all licence agreements;

5. Privacy and Monitoring
3.1 The GLC reserves the right(s) to:-
View any/all of the contents of the laptop.
View/access all transactions across the network.
View/access web history and emails

3.2 Illegal actions are covered by the following acts:
The GDPR (2018)
The Copyright, Designs and Patents Act (1988)
Obscene Publications Act (1959)
Theft Act (1968)

6. Technical Support
6.1. Students or their parents will not attempt to repair any faults. All faults must be reported to and repaired by the GLC ICT Systems team as soon as it is noticed;
6.2. Software support is limited to the software installed by the ICT Systems team.
6.3. It is the student's responsibility to ensure that their work is not lost due to mechanical failure or accidental deletion.
Please provide the email address of the parent/guardian accepting this contract, to receive a copy of your responses.

Email:_____

Student's First Name:_____

Student's Last Name:_____

Year Group of Student:_____

I have read the home school contract and agree to all parts outlined with regards to its usage, this includes returning the laptop and charger to the GLC school when my child leaves a GLC school.

Signed:_____