



Safeguarding Policy Addendum

Electronic Monitoring and Filtering at Charlton Park Academy

Appropriate filtering and monitoring on school/college devices and networks

The Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

Charlton Park Academy will do all we reasonably can to limit children's exposure to online harms through Academy provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place (Smoothwall system).

When implementing appropriate filtering and monitoring, Charlton Park Academy will ensure that "over blocking" does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach to online safety and we recognise that we cannot rely on filtering and monitoring alone to safeguard our students; effective safeguarding practice, robust policies, appropriate classroom/behaviour management and regular education/training about safe and responsible use is essential and expected.

Students will use appropriate search tools, apps and online resources as identified by staff after assessing student risks and special needs.

Internet use will be supervised by staff as appropriate to students' cognitive developmental age, ability and potential risk of harm.

Responsibilities

The Trust, alongside the Trust Principal & DSL has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed. The work in close conjunction with the Deputy Safeguarding leads to ensure the leadership team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.

Niall Fallon, DSL, and Mark Dale-Emberton, Principal and Steve Richardson, Safeguarding governors and Lynda Hage, chair of Governors, are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.

Our Senior Leadership Team are responsible for:

- procuring filtering and monitoring systems.
- documenting decisions on what is blocked or allowed and why.
- reviewing the effectiveness of our provision.
- overseeing reports.
- ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.
- ensuring the DSL and IT service providers/staff have sufficient time and support to manage their filtering and monitoring responsibilities.

The DSL has lead responsibility for overseeing and acting on:

- any filtering and monitoring reports.
- any child protection or safeguarding concerns identified.
- checks the filtering and monitoring system.

The IT team have technical responsibility for:

- maintaining filtering and monitoring systems.
- providing filtering and monitoring reports.
- completing technical actions identified following any concerns or checks to systems.
- working with the senior leadership team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.

All staff, students and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

Decision making and reviewing our filtering and monitoring provision.

When procuring and/or making decisions about our filtering and monitoring provision, our senior leadership team works closely with the DSL and the internet service providers/staff. Decisions have been recorded (IT helpdesk and web filter audit log) and informed by an approach which ensures our systems meet our Academy specific needs and circumstances, including but not limited to our student risk profile and specific technology use.

Any planned changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded (IT helpdesk and web filter audit log).

Our Academy undertakes an at least annual review, in conjunction with relevant Trust leaders of our filtering and monitoring systems to ensure we understand the changing needs and potential risks posed to our community.

In addition, on behalf of the Academy the Trust, the IT team alongside DSLs undertake regular checks on our filtering and monitoring systems, which are logged and recorded, to ensure our approaches are effective and can provide assurance to the Academy Board that we are meeting our safeguarding obligations.

Appropriate filtering

Charlton Park Academy's education broadband connectivity is provided by Smoothwall and LGFL as a comprehensive automated filtering and monitoring system.

Our Internet provider is a member of Internet Watch Foundation (IWF).

Smoothwall has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU).

Smoothwall filter is blocking access to illegal content including child sexual abuse material (CSAM).

Smoothwall filter blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.

We filter internet use on all Academy owned, or provided, internet enabled devices and networks. This is achieved by a purchased service - Smoothwall and LGFL filtering and monitoring which is installed on all devices.

Our filtering systems should allow us to identify device names or IDs, IP addresses, and where possible, individual users, the time and date of attempted access and the search term or content being blocked.

Our filtering system is operational, up to date and is applied to all users, including guest accounts, all Academy owned devices and networks, and all devices using the Academy broadband connection.

We work with our IT service providers/staff to ensure that our filtering policy is continually reviewed to reflect our needs and requirements.

If there is failure in the software or abuse of the system, for example if students or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to turn off monitor/screen, use a screen cover widget, report the concern immediately to a member of staff, and report the URL of the site to technical staff/IT team.

Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our child protection, acceptable use, allegations against staff and behaviour policies.

Parents/carers will be informed of filtering breaches involving their child.

Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported to relevant senior staff as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Metropolitan Police, NCA-CEOP or Royal Borough of Greenwich Children's Services.

If staff are teaching topics which could create unusual activity on the filtering and monitoring logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or leadership team who will liaise with IT services.

Appropriate monitoring

We will appropriately monitor internet use on all Academy provided devices and networks. This is achieved by our Smoothwall and LGFL filtering and monitoring systems.

All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

If a concern is identified via our monitoring approaches:

- Where the concern relates to students, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as child protection, acceptable use, and behaviour policies.
- Where the concern relates to staff, it will be reported to the Principal (or chair of governors if the concern relates to the Principal), in line with our staff behaviour/allegations policy.
- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Metropolitan Police via 101, NCA-CEOP, LADO or Royal Borough of Greenwich Children's Services.

Information security and access management

Charlton Park Academy is responsible for ensuring an appropriate level of security protection procedures are in place, in order to safeguard our systems as well as staff and students.

Charlton Park Academy will review the effectiveness of our procedures periodically to keep up with evolving cyber-crime technologies.

Mr Mark Dale- Emberton & Niall Fallon, members of the Senior Leadership Team are responsible for ensuring that our Academy has met the DfE cyber security standards for schools and colleges.

Remote/Online learning

Charlton Park Academy will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and any local/national guidance.

All communication with students and parents/carers will take place using Academy provided or approved communication channels; for example, Academy provided email accounts and phone numbers and/or agreed systems; Microsoft 365/Teams or equivalent.

Staff and pupils/students will engage with remote teaching and learning in line with existing behaviour principles as set out in our Academy behaviour policy/code of conduct and Acceptable Use Policies.

Staff and pupils/students will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

When delivering remote learning, staff will follow our Remote Learning Acceptable Use Policy (AUP).

Online Safety Training for Staff

Charlton Park Academy will ensure that all staff receive online safety training, which, amongst other things, will include providing them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring, as part of induction. Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding approach.

Educating students

Charlton Park Academy will ensure a comprehensive whole Academy curriculum response is in place to enable all students to learn about and manage online risks effectively as part of providing a broad and balanced curriculum.

Working with parents/carers

Charlton Park Academy will build a partnership approach to online safety and will support parents/carers to become aware and alert of the potential benefits and risks and to reinforce the importance of children being safe online.

Charlton Park Academy will ensure parents and carers understand that systems are used to filter and monitor their children's online use at Academy. Clarity will be ensured in terms of 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 is going to be interacting with online.

Where the Academy is made aware of any potentially harmful risks, challenges and/or hoaxes circulating online, national or locally, we will respond in line with the DfE 'Harmful online challenges and online hoaxes' guidance to ensure we adopt a proportional and helpful response.

Staff Engagement and Expectations

Staff awareness, induction and training

All members of staff have been provided with a copy of part one or annex A of the current version of 'Keeping Children Safe in Education' 2023 which covers safeguarding information for staff.

Academy leaders, including the DSL & DDSLs and governors/trustees will read KCSIE 2023 in its entirety. Leaders and all Academy members of staff who work directly with children will read annex B of KCSIE 2023. All members of staff have signed to confirm that they have read and understood the national guidance shared with them. (Forms evaluation)

It is a requirement that all members of staff have access to this policy and sign to say they have read and understood its contents. All staff are expected to re-read this policy at least annually (and following any updates) to ensure they understand our expectations and requirements.

All new staff and volunteers (including agency and third-party staff) receive safeguarding and child protection training (including online safety, which, amongst other things, will include ensuring an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) to ensure they are aware of the Academy Internal safeguarding processes, as part of their induction. This training is regularly updated and is in line with advice from the local safeguarding partners and explores the Greenwich processes to follow. All staff members (including agency and third-party staff) will receive appropriate child protection training (including online safety) that is updated at least annually, to ensure they are aware of a range of safeguarding issues and how to report concerns. Online safety training for staff will be integrated, aligned and considered as part of the whole Academy safeguarding approach and wider staff training and curriculum planning.

In addition to specific child protection training, all staff will receive regular safeguarding and child protection updates, at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

Charlton Park Academy recognises the expertise staff build by undertaking safeguarding training and from managing safeguarding concerns on a daily basis, and staff are encouraged to contribute to and shape Academy safeguarding arrangements and child protection policies.

All governors and trustees receive appropriate safeguarding and child protection (including online safety) training at induction. This training equips them with the knowledge to provide strategic challenge to be assured that our safeguarding policies and procedures are effective and support the delivery of a robust whole school approach to safeguarding. This training is regularly updated.

The DSL and Principal will provide an annual report to the Academy Governing Body detailing safeguarding training undertaken by all staff and will maintain an up-to-date record of who has been trained.

Approved by Governors: 18.10.24
Review Date: 17.10.25