IT Filtering and monitoring

Policy

My Choice School provides access to Microsoft365 and the internet access for use of all students and staff.

My Choice School aims to

- Have robust processes in place to ensure the online safety of students and staff
- Identify and support 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 school community in its use of technology, including use of mobile phones and when gaming outside of school
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content

- Exposure to illegal, inappropriate or harmful content including pornography, ignoring age ratings in games (exposure to violence, often associated with racist and misogynistic language), racism, misogyny and substance abuse
- Websites promoting self injury, suicide or eating disorders
- Hate sites including those promoting extremism in any form including antisemitism and radicalisation and undermining values of tolerance, respect, democracy, individual liberty and the law
- Validity of content, where authenticity and accuracy of content is in dispute.

Contact

- Being subjected to harmful online interaction with other users, such as peer-to-peer pressure and cyberbullying in all forms including trolling
- Commercial advertising
- Adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Identity theft including frape (hacking FaceBook, Instagram or other social media profiles) and sharing passwords

Conduct

- Privacy issues, including the disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (especially relating to the amount of time spent online)
- Any personal online behaviour that increases the likelihood of, or causes, harm to others
- Making, sending and receiving explicit images (consensual and non-consensual) also known as **SGII** (Self-Generated Indecent Images)
- Copyright (little care or consideration for intellectual property and ownership such as music or film)

Commerce

- Risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

This policy is based on the DfE statutory safeguarding guidance **Keeping Children Safe in Education** (September23) and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE **The Prevent Duty** guidance (September23) and The DfE guidance on **Meeting Digital and Technology Standards in Schools and Colleges** (January24)

Roles and Responsibilities

The **Head of Education** has overall responsibility for monitoring this policy and holding the **School Management Team (Head of Education DDSL, Headteacher DSL and Deputy Headteacher DDSL)** to account for its implementation.

The **Head of Education** 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 **Head of Education** will use the SMT meetings and the DSL meetings to discuss online safety, requirements for training, and monitor online safety logs.

The **Head of Education** will ensure that My Choice School has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Head of Education will review the DfE filtering and monitoring standards, and discuss with the My Choice IT Manager and school SMT any further action required to support the school 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.

My Choice School uses Schools Broadband as the Filtering and Monitoring Service.

The **Head of Education** DDSL will receive the Filtering and Monitoring reports from Schools Broadband and ensure that they are available for the Headteacher DSL and the Deputy Headteacher DDSL.

The My Choice IT Manager will provide technical; support and liaise with schools Broadband on technical issues.

The My Choice IT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, as directed by the Head of Education. These will be reviewed and updated at least annually to assess effectiveness and ensure students and staff are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly. This includes ensuring that there are systems in place for conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The **Headteacher and Deputy Headteacher** will ensure that all staff receive regular online safety updates in whole school meetings as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The **Headteacher** should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The **Headteacher** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headteacher DSL takes lead responsibility for online safety in school, in particular:

- Working with the Head of Education and the Deputy Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of Education to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the Head of Education and Deputy Headteacher teacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are recorded on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are recorded on CPOMS and dealt with appropriately in line with the school behaviour policy
- Working with the Head of Education and Deputy Headteacher to ensure that training is up to date and INSET training is delivered on online safety
- Liaising with other agencies and / or external services if necessary
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

An Acceptable Use Policy and Agreement is also in place to support appropriate and effective use of technologies for staff and students.

Teachers, Teaching Assistants and Behaviour Support Assistants

All school staff are responsible for:
Maintaining an understanding of this policy and implementing this policy consistently

- Agreeing and adhering to the My Choice School Acceptable Use Policy and Agreement and ensuring that students follow this
- Knowing who is responsible with the DSL for the filtering and monitoring systems and processes, and being aware that they need to report any incidents of those systems or processes failing by email
- Following the correct procedures by emailing the My Choice School Safeguarding Team (Head of Education DDSL, Headteacher DSL and Deputy Headteacher DDSL) if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are recorded and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

Parents and carers

Parents and carers are expected to:

- Notify the Head of Education, Headteacher or Deputy Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the Acceptable use Agreement
- To notify the Headteacher (in the first instance) or the Deputy Headteacher or Head of Education if they have any queries or concerns about online safety.

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre
- Hot topics Childnet International
- Parent resource sheet Childnet International

My Choice School will raise parents / carers' awareness of online safety in End of Day reports, telephone calls and emails, especially if there is a specific concern relating to their child. Parents will be informed if the school has concerns about online safety outside of school or if staff are aware that students have shared social media, online gaming or other contact details. This ensures that parents are aware of their child's online activities at home, including time spent online. This policy will also be available on the school website.

The school will let parents/carers know:

- What systems the school 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 school (if anyone) their child will be interacting with online

Visitors

Visitors who use the My Choice School IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

Educating Students about Online Safety

My Choice School recognises that social media and technology and are a part of every young person's life and the internet is an essential tool for accessing information, applying for jobs and courses and, in some instances, maintaining contact with family and friends.

Access to email for students is provided though Microsoft365 and student email traffic can be monitored by teachers. Access to email will be for the purposes of applying for college, employment or training opportunities.

The use of Microsoft365 and SharePoint is included in the Acceptable User Agreements.

Use of social media is not permitted on school technologies.

The Acceptable User Agreements also includes the management of mobile phones in school; all students must hand in their mobile phones (or other devices) and are not permitted to have these during the school day.

My Choice School recognises that students and other young people may be able to access social networking via smartphones, internet cafes, public Wi-Fi, libraries and via peers' devices regardless of whether they have been granted permission by their parent / carers. In recognising this is it is essential that all students (and parent / carers) are educated and empowered in recognising the risks and dangers associated with internet use. This is preferred to a 'locked down' approach where websites and access to technology has a blanket restriction and prohibition.

It is essential that all students and young people are able to take responsibility for their online communications and social media presence and understand and recognise acceptable and unacceptable behaviour in themselves and others. All students at My Choice School are taught about cyberbullying and staying safe online; this is regularly included as a topic in anti-bullying week and as part of assemblies. Cyberbullying is included in the My Choice School anti bullying policy.

Open dialogue is encouraged in order to address concerns about online presence, profile and safety. Online safety education must be proactive and reactive and must ensure that students develop the following skills, knowledge and behaviours:

- To STOP and THINK before they CLICK
- To develop a range of strategies to evaluate and verify information before accepting its accuracy
- To be aware that an author of a website or page may have a particular bias or purpose and to develop skills to recognise what they might be
- To know how to narrow down or refine a search
- To understand how search engines work and to understand that this affects the results they see at the top of the listings
- To understand acceptable behaviour when in an online environment such as no abusive language, keeping personal information private
- To understand how photographs can be manipulated and how online content can attract the wrong sort of attention
- To understand why online 'friends' may not be who they say they are and to understand why they should take care in online environments
- To understand why they should not post or share detailed accounts of their personal lives, daily routines, locations, contact information, photographs and to ensure they know how to adjust privacy settings
- To understand that they must not post photographs or videos of others without their permission
- To understand how and why some people will groom young people for sexual or other criminal reasons
- To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by online bullying
- To know how to report any abuse and how to seek help if they are experiencing any difficulties with cyberbullying on any device or technology

The My Choice School curriculum also includes online safety, in PSHE and SRE.

In **KS3**, students 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

In **KS4**, students will be taught to:

- 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

By the **end of KS4**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Students and young people will be reminded about their responsibilities and all staff and teachers are expected to model safe and responsible behaviour in their own use of technology during working hours and in the classroom.

In addition all students must be supervised by a member of staff when online or using the computer in the classroom; whether in school hours or not.

To further ensure responsibility and fairness in accessing the computer in the classroom the following rules also apply, in addition to the Acceptable Use Agreement:

Conditions of computer use in the classroom

- Students must be supervised while using computers and accessing the internet.
- Students accessing the internet and email must remember that they are representatives of My Choice School and must not engage in any activity which is illegal or likely to cause offence or disruption to the system.
- Students must not download material or introduce software without permission from the teacher.
- The computers in the classroom are for use of My Choice School students and teachers for school work. Any access for use other than school work must be agreed by the teacher.
- Music must not be played as entertainment as this contravenes any licensing or broadcast prohibitions.
- Social media or other social networking may not be accessed on the classroom computer during the school day.
- My Choice School students and other young people should respect each other’s computer time and not interrupt.
- My Choice School students and other young people must not trespass into other users’ files or folders.

All students (and staff) must sign the Acceptable Use Policy and Agreement.

Policy Link:

My Choice School Antibullying
My Choice School Safeguarding
Employee handbook: use of email, internet and social networking
Acceptable Use Policy and Agreement for Staff
Acceptable Use Policy and Agreement for Students.

Computer and Internet Policy:
Reviewed May 2021
Reviewed May 2022

Reviewed May 2023

IT Filtering and Monitoring Policy (incorporating and replacing the Computer and Internet policy) January 2024

Annual Review due June 2024