Slough and Eton Church of England Business and Enterprise College

A Member of Slough and East Berkshire C of E Multi Academy Trust

e-Safety Policy

Owner:	Mrs Catherine Goodyear
Ratified by Governing Body:	
Date Ratified:	October 2026
Date Policy to be reviewed:	Autumn 2027

Contents

1. Aims 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating students about online safety 6
5. Educating parents/carers about online safety 7
6. Cyber-bullying 7
7. Acceptable use of the internet in school 9
8. Students using mobile devices in school 9
9. Staff using work devices outside school 9
10. How the school will respond to issues of misuse 10
11. Training 10
12. Monitoring arrangements 11
13. Links with other policies 11
Appendix 1: Home School Agreement (students and parents/ carers) 12
Appendix 2: Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors) ……...13

---

1. Aims

The school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of 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 school 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 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** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, 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 Education, Relationships and Sex Education and Health Education guidance
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteacher 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), 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 co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the co-designated safeguarding leads (Co-DSLs) and the Strategic Safeguarding Lead.

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

The governing body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. Governors will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those 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 governor who oversees online safety is Kiran Jhanzaib

All governors will:

- Ensure they have read and understand this policy

- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some 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

3.2 The headteacher

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

3.3 The strategic safeguarding lead

Details of the school's strategic safeguarding lead is set out in our Child Protection and Safeguarding Policy. The strategic safeguarding lead oversees the Safeguarding Team (which comprises of the Co-DSLs, the Strategic Safeguarding Lead and the Deputy DSLs), staff training about online safety matters, information dissemination regarding online safety to all stakeholders, identifying trends and patterns that require action from the school, leading the school's response to online safety, and formulating policies that are related to online safety. The strategic safeguarding lead is responsible for:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Network Manager to make sure the appropriate systems and processes are in place
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face using the LGFL Online Safety Audit & Risk Assessment https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fviewonline.lgfl.net%2Fhubfs%2FSafeguardED%2FOnline%2520Safety%2520Audit%2FLGfL-Online-Safety-Audit-2025-v3.1.docx&wdOrigin=BROWSELINK
- 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

This list is not intended to be exhaustive.

3.4 The co-designated safeguarding leads

Details of the school's co-designated safeguarding leads (Co-DSLs) (and deputies) are set out in our Child Protection and Safeguarding Policy.

The Co-DSLs take lead operational responsibility for online safety in school, in particular:

- Working with the headteacher, Network 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 and Safeguarding Policy
- Ensuring that any online safety incidents are logged on Securus and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school Behaviour for Learning Policy

- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

3.5 The Network Manager

The school's Network Manager is Matt Kettley. The Network 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, which are reviewed and updated at least annually to assess effectiveness and ensure students 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
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Knowing that the strategic safeguarding lead is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by emailing safeguarding@slougheton.com.
- Following the correct procedures by informing helpdesk@slougheton.com if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the Co-DSLs to ensure that any online safety incidents are logged 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'

This list is not intended to be exhaustive.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/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
- Parent resource sheet – Childnet

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships and sex education and health education in secondary schools

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

Students in **KS4** will be taught:

- 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 secondary school**, students 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)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to cryptocurrency and / or online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online, how to be a critical thinker by maintaining the thought of "could this be AI".

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home such as WEDUC, the weekly Parent Communication, and in information via our website. This policy will also be shared with parents/carers.

Online safety will also be covered during parents' evenings.

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

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher, the strategic safeguarding lead and/or the Co-DSLs.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's behaviour for learning policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form Tutors, PHSE teachers, and Computing teachers will discuss cyber-bullying with their groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

A Co-DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so (usually a member of the Senior Leadership Team) by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or 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 students and staff. If the search is not urgent, they will seek advice from the headteacher or a Co-DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members 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 headteacher and/ or the Co-DSL 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 student 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 a Co- DSL (or a Deputy DSL) immediately, who will decide what to do next. The Co-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 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 for Learning Policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as those provided by Microsoft Copilot, ChatGPT and Google Gemini.

The school recognises that AI has many uses to help 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 school will treat any use of AI to bully students in line with our Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

7. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 & 2). 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 & 2.

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during:

- Lessons, unless permission has specifically been given
- Tutor time, unless permission has specifically been given
- Clubs before or after school, or any other activities organised by the school, unless permission has specifically been given

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student will trigger disciplinary action in line with the school Behaviour for Learning Policy, which will result in the confiscation of their device.

9. Staff using work devices outside 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 can be made up of 3 random words, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol) if required, or generated by a password manager
- Ensuring their 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
- Keeping the device in a secure place when it is not in use.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- 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, as set out in appendix 2.

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 helpdesk@sebmat.com

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on Behaviour for Learning and the School IT Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures / staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

11.1 Staff, governors and volunteers

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 relevant updates as required (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, 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 students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The Strategic Safeguarding Lead, the Co-DSLs (and deputies) will undertake 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 will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

11.2 Students

All students will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Students will also receive age-appropriate training on safeguarding issues such as AI usage, cyberbullying and the risks of online radicalisation.

12. Monitoring arrangements

The school uses broadband connectivity through the London Grid for Learning.

The school uses London Grid for Learning web filtering which blocks sites that are categorised as harmful to children, including those listed by the Internet Watch Foundation.

The school uses SECURUS to monitor usage of school-based devices. A monthly report is read by the Strategic Safeguarding Lead who follows up on key individuals of concerns and also on overall trends and emerging patterns. Serious incidents (for example attempts to research suicide or bomb making) are telephoned directly to a Co-DSL by SECURUS and these are dealt with immediately.

The Strategic Safeguarding Lead and the Co-DSLs log safeguarding issues related to online safety on CPOMs. Behaviour issues related to online safety are logged on Class Charts by the member of staff who dealt with the incident (usually the class teacher).

This policy will be reviewed every year by the Strategic Safeguarding Lead. At every review, the policy will be shared with the governing body. The review will be supported by an annual risk assessment (as mentioned on Page 4) that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour for Learning Policy
- Centre Quality Assurance Handbook, Vocational Provision/ NEA
- Disciplinary Policy Procedure
- Exams Policy
- Complaints Procedure for School
- School IT Acceptable Use Agreement
- Data Protection and Security Policy (SEBMAT)

Appendix 1: Home School Agreement (including E-Safety Guidelines)

Home School Agreement

Slough and Eton Church of England Business and Enterprise College recognises that the partnership between home and school is vital to ensure the success of every student.

Students. To achieve the best possible outcomes, students agree that they will:

Work Hard

- work hard in class and meet all deadlines for handing in independent study.
- take an active part in school life including attending extra-curricular clubs and lessons.

Be Nice

- show respect and care for others and their property.
- report any concerns about the safety and behaviour of other students.
- accept and respect all students and staff, regardless of their ethnicity, gender (including transgender), sexuality (LGBTQ+), disability, age or religion.

No Excuses

- attend school regularly and arrive at registration on time with the right attitude for learning.
- wear school uniform correctly and bring the correct equipment each day.
- behave well in and out of class and meet all the school's expectations including on the journeys to and from school and on any trip or visit.
- be responsible for all their possessions and not bring into school expensive items or large sums of money.
- talk with parents & teachers about any concerns in school and pass all letters and notes to parents on the day they are issued.
- adhere to the behaviour, bullying and e-Safety Policy.

Student Name: ..... Form Group: ..... Signed Student:.....

Parents. To achieve the best possible outcomes for our students, parents agree that they will:

- support school policies and see that their child attends school regularly, on time and is properly equipped.
- take an active interest in all aspects of their child's school life.
- communicate to school all relevant information which may affect their child's work or attitude to learning.
- notify the school if, for any reason, their child cannot attend school.
- ensure their child follows the school's behaviour policy and support associated action taken by the school.
- encourage learning outside of school, provide suitable facilities to learn, and encourage their child to have the right attitude to learning.
- encourage their child to accept and respect all students and staff, regardless of their ethnicity, gender (including transgender), sexuality (LGBTQ+), disability, age or religion.
- attend Parents' Evenings, student support meetings and other occasions at which their presence is required.
- Ensure the school has up to date contact details, medical information and other barriers to learning about their child.

Signed Parent: .....

Slough and Eton. To achieve the best possible outcomes for our students, the school will:

- provide a safe and stimulating environment for all your children to learn.
- offer a broad and balanced curriculum to students of all abilities.
- encourage all students to take responsibility for their own learning, feel proud of their achievements and enjoy being a student at the school.
- keep parents/carers informed about their progress and general school matters.
- insist that all students observe the school's behaviour and anti-bullying policies.
- provide an environment where all students are accepted with respect regardless of their ethnicity, gender (including transgender), sexuality (LGBTQ+), disability, age or religion, and challenge all prejudice when it occurs
- act without fear or favour with safeguarding concerns, placing the child at the centre of our decision making.
- set regular independent study and provide suitable facilities at school.
- assess students' work and provide regular targets and guidance on how to improve.

Signed on behalf of the School: .....

I have come in order that you might have life – life in all its fullness

Work Hard Be Nice No Excuses

M Culkeen 02/01/24

E-Safety Guidelines

With regard to the use of the school's IT systems students will:

- ensure their IT usernames and passwords are safe and secure – they will not share them, nor will they try to use any other person's username and password.
- not disclose or share personal information about themselves or others when online.
- immediately report any unpleasant or inappropriate material or messages or anything that makes them feel uncomfortable if they see it online.
- not use the school systems for personal or recreational use (including e-mail) unless they have permission.
- not use the school systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g., YouTube) unless they have permission.
- not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- be polite and responsible when they communicate with others.
- not take or distribute images of anyone without their permission.
- only use their own personal devices (mobile phones, USB devices etc.) in school if they have permission and in accordance with school policies.
- not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others.
- not try to use any programmes or software that might allow them to bypass the filtering or security systems or cause damage or disruption to the school system.
- immediately report any damage or faults involving equipment or software.
- not tamper with, disconnect, attempt to repair or damage school equipment.
- not install, attempt to install or store programmes of any type on any school device, nor will they try to alter computer settings.
- only use social media sites with permission and at the times that are allowed.
- ensure that they have permission to use the original work of others in their own work.
- will not try to download work which is protected by copyright (including music and videos).
- understand submitted work will be passed through "Turn It In" and plagiarised work will be retuned with a possible sanction.
- not use Artificial Intelligence (AI) to complete work. Students doing this may be sanctioned.
- understand the IT system is monitored and infringements of these guidelines will be investigated and sanctioned.

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

SCHOOL IT ACCEPTABLE USE AGREEMENT

For my own personal safety:

- I understand that the School will monitor my use of the systems, devices and digital communications.
- I will keep my usernames and passwords safe and secure – I will not share them, nor will I try to use any other person's username and passwords. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the School systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the School has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the School:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not tamper with, disconnect, attempt to repair or damage school equipment.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action that could result in dismissal in the event of illegal activities/ involvement of the police.

Advice to staff: what to do if there is a malware or virus attack

It is always a possibility that something will slip through our defences, as it's not possible to be 100% secure. If you notice an issue such as random pop-ups and warnings, notice files are disappearing or changing icons, or see a ransomware pop-up, it is vital that you stop what you are doing, and do not press any buttons on the keyboard or click anything on the screen. **Crucially, DO NOT switch off the machine**.
Please contact Matt **immediately** as follows:
Slough and Eton: Matt Ketteley – mke@slougheton.com – extension 2301
If Matt is unavailable, contact Ian Trevena directly on 07854 157504
Please be vigilant – you form part of our security team as well, and we can stop most things together.