READING BLUE COAT

E-Safety, Digital Communications, and Student Device Policy

1. Introduction

1.1 Context: The internet and digital communication are essential to and have transformed business and social interaction in the contemporary world. The growth of Artificial Intelligence (A.I.) is revolutionising society and the economy in ways that are difficult to predict. Reading Blue Coat (RBC) therefore has a duty to provide students with quality, safe access as part of their learning experience, to ensure safety, raise educational standards, promote achievement and support the professional work of staff. We encourage our students to enjoy using the internet and digital tools in a responsible way, not forgetting that they are accountable for any media that they produce or share via online platforms and services. Digital safety is the responsibility of all those involved in the life of the School, including parents.

1.2 School values: The following policy is intended to support the five key values of RBC, for example:

- **Aspiration** – aiming for excellence in the use of technology.
- **Compassion** – to leverage technology to support and help others.
- **Courage** – to identify and confront misuse or online abuse.
- **Integrity** – acknowledging and rectifying the consequences of misuse.
- **Service** – enabling connections with the local community and wider world.

1.3 Scope: This policy applies to all members of the RBC community (students, staff, volunteers, Governors, parents) with respect of their use of the School's IT resources, accounts, and connections, and the use of personal devices and resources onsite. Policies are also applicable to the conduct of students and staff outside of School, which may include an element of online behaviours, and so this policy must be read in conjunction with the associated policies identified at the end of this policy document.

2. Roles and responsibilities

2.1 The Governors will:

- Review and approve the *E-Safety, Digital Communications and Student Device Policy* annually.
- Request and review information for the monitoring of e-safety at RBC.
- Ensure that there will be a designated Governor with responsibility for filtering and monitoring standards. This will be the Safeguarding Governor.
- Ensure that there are clear roles and responsibilities for filtering and monitoring among school staff and third parties (e.g., external service providers).
- Ensure the relevance of this policy to contemporary technology, including the development of A.I.

2.2 The Headmaster will:

- Promote a clear agenda for e-safety and appropriate digital conduct as part of the wider aims and ethos of the School.
- Understand and implement this policy and related policies in respect of allegations against staff, low level concerns, and any student behaviour or welfare concerns of sufficient seriousness to be referred to the Headmaster.

2.3 The Designated Safeguarding Lead will:

- Review, revise, and present this policy annually for Governor ratification.
- Provide information to Governors as per their requirement.
- Ensure good levels of training for the DSL, Deputy DSLs, and other staff, and ensure that all staff understand their role, follow policy and procedure, and act on any concerns.
- Ensure the implementation of this policy and related policies that are relevant to online safety and welfare.
- Manage safeguarding cases that arise as a result of online behaviours.
- Actas the designated member of SLT with responsibility for filtering and monitoring.
- Liaise with the Network Manager to manage e-safety and security (including filtering and monitoring) on the School's network.
- Chair a meeting (at least once per term) with the Network Manager to: discuss procurement of filtering and monitoring systems, document decisions about what is blocked or allowed and why, review the effectiveness of the School's provision, and oversee reports relating to this domain.
- Ensure that minutes from these meetings are shared with Governor when required.
- Liaise with the Deputy Head (Education Development) to ensure the suitability and safety of use of A.I. for education purposes.

Ensure that the standards from Government Guidance (*Meeting Digital and Technology Standards in Schools and Colleges*, DfE, 2023) are used as a review checklist in regular meetings.

2.4 The Network Manager will:

- Proactively monitor the use of School networks, accounts, and resources to ensure appropriate e-safety and conduct.
- Hold technical responsibility for filtering and monitoring systems, providing reports, and completing actions following concerns or checks.
- Ensure that those systems meet the technical requirements set out in Government guidance and standards.
- Ensure that technical checks are carried out on a regular basis, which encompass a range of devices, locations, and user types, and are recorded in a log that includes: when checks took place, who did them, what was checked, and resulting actions.
- Report concerns regarding student behaviour to the appropriate pastoral staff.
- Report safeguarding and welfare concerns to the DSL.
- Liaise and participate in regular meetings with the DSL to manage e-safety and security on the School's network. The Network Manager will be responsible for bringing technical expertise and proposals to these meetings.
- Ensure that other members of IT staff reporting to the Network Manager are aware of and effective in identifying and reporting concerns.
- Attend Governors' Safeguarding Committee annually, to enable strategic review of the School's approach to filtering and monitoring, and network security.

2.5 The Deputy Head (Academic) will:

- Identify and publish requirements for student devices in classrooms and other learning activities.
- Liaise with other members of SLT to ensure academic use of technology is consistent with the School's aims for the welfare and behaviour of students.

2.6 The Deputy Head (Education Development) will:

- Provide guidance and training to staff, to ensure that the use of A.I. for academic purposes is consistent with the School's values and with best practice for safeguarding, behaviour management, data protection, and achieving educational aims.

2.7 All Staff will:

- Understand and adhere to this policy and related policies, to ensure appropriate and safe online behaviours.
- Report any online related welfare, behaviour, or safeguarding concerns as per the School's other policies.
- Ensure that all digital communications are appropriate and professional.
- Promote the value of safe and appropriate online behaviour among students.
- Maintain a realistic and up-to-date awareness of how students use devices and the risks associated with that usage.
- Report any concerns about filtering and monitoring, and network security promptly, via email, to: the Network Manager and DSL. This will include any of the following cases:
    - they witness or suspect unsuitable material has been accessed
    - they can access unsuitable material
    - they are teaching topics which could create unusual activity on the filtering logs
    - there is failure in the software or abuse of the system
    - there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
    - they notice abbreviations or misspellings that allow access to restricted material

2.8 All Students:

- Are responsible for using the School's IT systems in accordance with the *Acceptable Use Policy*.
- Should understand research skills, and the need to avoid plagiarism and uphold copyright regulations.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices.
- Will be expected to know and understand policies on the taking/use of images, on the use of A.I., and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's *E-safety, Digital Communications and Student Device Policy* covers their actions out of school, if related to their membership of the School.

2.9 Parents/guardians:

- Parents/guardians play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The School will take every opportunity to help parents understand these issues through, for example:
    - Parents' seminars
    - Resource provision
- Letters, social media and information about national/local online safety campaigns/literature (e.g. www.swgfl.org.uk, www.saferinternet.org.uk, www.childnet.com/parents-and-carers, 'ThinkUKnow' parents' website (which is run by the National Crime Agency) and the 'Safer Schools' app (available through Apple or Android) – our access code is 7675.). Parents and guardians will be encouraged to support the School in promoting good online safety practice and to follow guidelines on the appropriate use of:
    - o digital and video images taken at school events
    - o access to the Parent Portal and online student records
    - o their children's personal devices in the School

3. E-Safety and education

3.1 Educational aims for digital technology and internet use: Electronic information-handling skills are fundamental to the preparation of citizens and future employees. The School encourages digital and online activities that:

Investigate and research subjects, cross-curricular themes, or topics related to social and personal development.
Support intellectual curiosity, individual research projects, academic extension.
Investigate careers and Higher Education.
Develop students' competence in ICT.
Enable better communication and more efficient participation in enriching activities, such as the arts, sport, or adventure education.
Promote good conduct, welfare, and a sense of community.

3.2 Educating students about e-safety and appropriate communication: Students are taught about the importance of safe and appropriate use of the internet and digital tools using the following means:

- A curriculum in Wellbeing & Futures (PSHE) lessons that is carefully mapped to be both comprehensive and age appropriate.
- Programmes of assemblies and tutor sessions that are set out by Directors of Section and Heads of Year.
- Pastoral talks by expert speakers that are arranged by the Director of Wellbeing & Futures).
- Communications with the Digital Council (see further point 7, below).
- Guidance documents published to students.

The School follows the non-statutory guidance, *Teaching Online Safety in Schools* (2023) to further ensure the quality and appropriateness of its provision.

3.3 Key elements covered in the education of students: A wide range of topics and messages are communicated to students via the means identified above. This policy does not provide an exhaustive list, but key elements that the School's provision will cover include:

- Critical awareness of materials that can be found online – their accuracy, validity, safety, and appropriateness.
- Understanding of the benefits and risks of social media and other forms of online communication with peers and others.

- Understanding the benefits and risks of A.I. technologies, including how they may be used appropriately for academic purposes, the wider potential benefits to society, and the risk factors associated with abusive, illegal, and unethical use.
- The role that online communication plays in wider safeguarding concerns, such as grooming or sharing of images.
- The role of digital media and data in wider society and economy and how management of a digital footprint can affect later life.

3.4 Educating staff: It is essential that all staff receive online safety training, and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- E-safety training will be embedded in the annual staff training programme. Established issues and new or evolving online harms will be covered in the annual safeguarding training, delivered to all staff at the beginning of each academic year.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the *E-Safety, Digital Communications and Student Device Policy* and *Acceptable Use Policy*.
- All staff are expected to undertake dedicated training focused on online safety (typically, in the form of an e-learning course) and will be required to refresh such training regularly by the DSL.
- It is expected that some staff will identify online safety as a training need within the PDR process.
- Staff will receive specific guidance from the Deputy Head (Education Development) on the appropriate use of A.I. for academic purposes, so that they may guide students in safe and effective use of such technologies in the classroom and in homework.
- The DSL (or other nominated person) will receive regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations
- This *E-Safety, Digital Communications and Student Device Policy* and its updates will be presented to staff as part of ongoing training and feedback will be sought.
- The DSL (or other nominated person) will provide advice/guidance/training to individuals as required.

4. Systems, devices, mobile phones

4.1 Use of School hardware and network: Access to the internet may be provided via School computers and networks, and wireless connections. School devices are chiefly located in designated computer rooms. Guidelines for appropriate use of the internet are posted near all computers and in every form room. Students and staff are required to read and accept the School's *Acceptable Use Policy (AUP)* before making use of the School's devices and networks. Access to School networks and accounts is given via a personal login for each student or member of staff, which is password protected. Passwords should be secure and routinely updated. The Network Manager ensures that anti-virus software is utilised and updated, to protect systems and users.

4.2 Monitoring, filters, and blocking: The following measures are taken to ensure safety and appropriateness of the School's systems, networks, accounts:

- The Network Manager continually reviews the safety and security of IT systems, the means by which they are monitored, and liaises with SLT to develop and improve the technical side of e-safety.

- Monitoring includes both the physical monitoring of student screens by any staff supervising and the remote monitoring of internet access through any software/third party solutions employed by the School.
- The Network Manager and DSL monitor students use of the School's network, including communications via email and Teams. Any messages sent via school systems could potentially be shared with members of SLT.
- The School will filter and block access to some online resources via its network – judgements are made in consultation by the Network Manager and the DSL. These judgements will consider the balance of online safety without unreasonably impacting teaching and learning, or restricting students from learning how to assess and manage risk themselves. Students may from time-to-time require access to a site that is blocked for some legitimate academic purpose. Access to such sites via the School's networks will only be given by written permission from the DSL and the rationale will be recorded.
- It should be noted that monitoring of internet access also applies to any personal devices using the School's Wi-Fi.
- External systems will generate 'alerts' for unsafe or inappropriate online activity by users. These alerts will be monitored during school hours by the DSL, Headmaster and the Network Manager. Any urgent concerns will receive a prompt response. Members of staff may see alerts outside of school hours (evenings, weekends, holidays) and will respond when possible, but there is no expectation of a 24/7 response from staff.

4.3 Student laptops: All students are required to bring a laptop each day (including compatible headphones and charger) for academic purposes. Further technical requirements will be agreed and advertised from time-to-time by SLT, and reasonable notification given to parents. Laptops must be able to access School accounts and internet resources (for example, Microsoft Teams). To ensure good levels of e-safety and appropriate use, supervising staff will:

- Advise students during lessons and activities as to what is (and is not) correct use of the laptop for the designated task.
- Proactively monitor what students are doing on their devices; intervene when necessary.
- Report inappropriate use to pastoral staff (Head of Year, in the first instance).
- Where appropriate, review what a student is accessing or doing more closely – e.g., asking to see tabs open on a browser, reading a Teams chat thread.
- Laptops should not be connected to the internet via VPNs or hotspots, as these circumvent the School's filtering and monitoring systems. If discovered, the member of staff should ask the student to stop immediately and report promptly to the student's Head of Year.
- The School is gradually implementing an expectation (started in September 2025) that new students in Year 7 purchase laptops through a managed scheme; such devices will include pre-loaded safety systems, and will be monitored and managed by RBC staff as needed.

4.4 Mobile phones and other devices: Students are permitted to bring mobile phones to School each day as they have a legitimate purpose (e.g., communicating with parents about transport arrangements). However, their use at RBC is strictly regulated:

- Students in Years 7, 8, 9, 10 & 11 are not permitted to use their mobile phones during the School day. The expectations is they will be placed in the student's Yondr pouch until the end of the School day. If students need to call home due to an emergency, they may request permission to do so from a member of the Lower or Middle School teams. This helps the staff to monitor pastoral concerns.
- Students in Years 12-13 may use their mobile phones in the Sixth Form Centre or Annexe, or on the direct instruction of a member of staff. They must be switched off during academic lessons, study periods and whilst using the Library.

These policies regarding phones are further set out in the RBC *Student Manual.*

Students are asked not to bring other electronic devices into School (e.g., gaming devices, speakers) unless for a specific purpose agreed by staff. If found, these devices may be confiscated and sanctioned by staff as per mobile phones.

It is to be acknowledged that the widespread use of smartphones has meant that student access to the internet may have very few (if any) restrictions. The School's wireless network is strictly regulated, but students may access online services via mobile data. Therefore, staff are asked to be vigilant and aware of the significant risks that smartphones may pose. It is good practice to have open conversations with students about what they are accessing via smartphones and report pastoral concerns to Heads of Year. Depending on the nature of any content accessed, it may be necessary to follow the School's *Child Protection & Safeguarding Policy*. It is appropriate to challenge and confiscate, should a member of staff be sufficiently concerned by what a student is doing. Rarely, a mobile phone may be subject to a longer confiscation and search, but in such cases the rationale must be clearly recorded and communicated to the student and their parents (unless given specific advice to the contrary by the Police or other external agencies). Searches of devices will only be conducted in accordance with the School's *Searches & Confiscation Policy*. It is reasonable for a member of staff to look at a student's screen and activity during a lesson, and this alone does not constitute a 'search'.

5. Digital communications

All students and staff will regularly communicate digitally, via School accounts; email and Microsoft Teams messages are widely used and legitimate means of communication. The careful use of passwords and secure devices is expected of all users, to ensure secure and appropriate communications.

5.1 Communication between students and staff: Communications should be appropriate and strictly limited to School accounts. Further details and expectations are set out in the RBC Staff Code of Conduct. Not only the means, but also the tone and language of communication should be appropriate, and staff have a responsibility to help students choose the right language and presentation of messages. Staff and students may 'chat' over Teams, but staff must ensure that over-familiarity or blurred boundaries are carefully avoided. Should any communication worry a member of staff, they should report it to the DSL for further advice.

5.2 Expectations of students: Students are expected to check their emails and Teams messages daily, at the start of the School day, at 14:00 and after school, and respond appropriately. They should not use school systems as an informal means of communication among their peer group. Students are asked to report any concerning behaviour or content to their Tutor and Head of Year. Students should use polite and appropriate language in drafting messages; persistent and deliberate inappropriate communication will be escalated as a behavioural matter. Further guidance as to the boundaries and management of communication will be published to students from time-to-time, to ensure consistent, safe, and reasonable usage.

- There is an electronic messaging amnesty from 19:00 on weekdays during term time. If a Teams message or email is sent after 19:00, then the sender should not expect a member of staff to see it until the following day. Teachers may still respond in the evening depending on the type of question being asked. Like any query, it may need a very quick response or something more detailed the following day.

- Electronic messages received after 19:00 on a Friday during term time week will be responded to by close-of-business the following Monday. Again, the teaching staff can exercise their judgement depending on the nature of the query, for instance if it concerns co-curricular activities over the weekend.

- Electronic communication in the holidays is at the teacher's discretion. Some communication might be desirable in the run up to mock or summer exams. Therefore, in an academic context, the teaching staff will make every effort to ensure that instructions and resources are clearly set out at the end of a term to limit the need for further communication in the holiday.

- Pastoral/safeguarding concerns are exceptions to the time limitations described above, as issues may occur during evenings and weekends. However, it is best for personal or sensitive communication not to remain on Teams, where a discussion in person at School would be the most appropriate. If a member of staff is contacted through Teams about a pastoral/safeguarding concern, they will contact the Safeguarding Lead and/or SLT member on duty as soon as possible. Discussions between students and staff (typically, pastoral staff) about safeguarding concerns may take place on Teams where there is an urgent need.

- Messaging in Teams should be polite, formal and start with 'Hi or Dear Mrs/Mr and a **surname**'. Once the communication thread is established, comments do not need to be prefaced with 'Mr/Mrs and a surname'. We believe that these are good communication habits for our students to be in.

6. Behaviour and welfare online

As a general and guiding principle, all users should expect to maintain the same, high levels of behaviour in online interactions that they would use face-to-face. There is a risk that online communication may lead to some students feeling less inhibited or aware of the impact of their actions online, and therefore it is important for the School to take a proactive role in educating and challenging as issues arise.

Following the 2021 OFSTED *Review of Sexual Abuse in Schools and Colleges*, it is important for all staff to operate with the understanding that sexual abuse (including online sexual abuse, and abuse enabled by A.I.) is pervasive in our society will affect students at RBC. Students may be the instigators of such abuse, complicit in it, or be the target for abusive behaviour and communications. To that end, it is crucial that staff engage with students with a sense of realism and awareness, as well as compassion, and understand that concerns for e-safety are thoroughly enmeshed in issues of Child Protection and Safeguarding. All staff are asked to read this policy in conjunction with the *Child Protection and Safeguarding Policy* to gain a holistic understanding of how to support young people in staying safe online.

6.1 General principles: The School reserves the right to make decisions as per the circumstances and impact as to which online behaviours count as harmful or inappropriate. However, as a non-exhaustive list, students are not permitted to:

- Retrieve, store, send, copy, or display offensive or harmful messages or media.
- Use A.I. technologies to generate offensive or harmful media.
- Use A.I. technologies to exploit and or manipulate media (e.g., images) or another person, or misuse their data, personal information, or intellectual property (including the School's).
- Use discriminatory language.
- Harass, insult or attack others, or incite another person to do so.
- Assume false identities, mislead, or use anonymity to harm others.
- Damage computers, computer systems or computer networks, or the devices of other members of the community.
- Ignore copyright laws or use technology for academic dishonesty.
- Compromise or use another user's password or other secure information.
- Go into another user's folders, work, files, or any other data.

- Exploit or steal online resources for financial gain or misuse.
- Use the School's network or accounts for commercial purposes.
- Participate in, promote, encourage, or glamorize any illegal activity, or activities that are contrary to the School's values or rules.

It should be noted that a number of the actions above, depending upon their precise nature and severity, may require that the School makes a report to the Local Authority and/or the Police.

6.2 Cyberbullying: Cyberbullying is a pernicious form of bullying because it can be so pervasive and potentially anonymous. There can be no safe haven for the victim who can be targeted at any time or place. Cyberbullying could involve communications by various electronic media, including for example:

- Texts, instant messages or calls on mobile phones;
- The use of mobile phone camera images to cause distress, fear, or humiliation, and the use of A.I. tools to exploit such media in a harmful way;
- Posting threatening, abusive, sexual, discriminatory, offensive, or humiliating material or comments on websites (including blogs, personal websites, and social networking sites such as Snapchat, Tik Tok, Facebook, Instagram, X, or YouTube);
- Using e-mail to message others in a threatening or abusive manner; or
- Hijacking/ cloning email accounts.

The School's *Anti-Bullying Policy* describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying. The following points summarise the RBC approach to cyberbullying:

- RBC employs preventative measures to reduce the risk of cyberbullying:
    - It requires all students to adhere to this policy and the *Acceptable Use Policy*
    - It utilises filtering and monitoring systems to intercept harmful comments and content
    - It employs disciplinary measures to deter cyberbullying
    - It issues student users with their own network accounts and email addresses, and expects all communication to occur through official accounts that can be monitored
    - It provides guidance on safe internet use and social media in Wellbeing lessons
    - It provides a phone-free environment for Years 7-11 and restricts access to phones ('not seen') for Sixth Form
    - It takes seriously breaches of the phone policy, including use of phones in toilets and changing rooms
- Education of students to ensure that they have a good understanding of the risks of cyberbullying, that it could happen to anyone, and that there are effective means to respond to it. Students should be encouraged to come forward and understand that they are not alone. Good relationships and open communication with staff (tutors, Heads of Year) will enable a flow of information about online behaviours that can reduce the risk of cyberbullying.
- RBC communicates a strong message of equal respect and inclusion for all, and students are expected to buy-into that message as 'active bystanders' to harassment and bullying, advocating for one another and notifying staff when worried about their peers or friends.
- Students are given different options to communicate their concerns or report that they are being cyberbullied – in person, via digital messages (email, Teams, etc.), anonymously (using the Worries boxes on site or online Worried Form on RM Unify), etc. This makes it easier for them to come forward and feel secure in sharing information.
- The response to cyberbullying is consistent with any other form of bullying – it is not tolerated, is contrary to the School's values, and so may lead to significant sanctions in accordance with the *Behaviour, Rewards and Sanctions Policy*, *Anti-Bullying Policy* and *Student Manual*. Sanctions are decided on a case-by-case basis and may be more or less severe based on context. Established cases of cyberbullying will always receive a significant sanction (a detention or exclusion) and

may be in some cases by classified as 'child-on-child abuse'. This deters cyberbullying and reinforces the message that it is wrong.
- Students are informed about online tools for countering cyberbullying during Wellbeing and Futures lessons – for example, using block functions, reporting tools, etc.
- Where cyberbullying becomes a safeguarding issue, the *Child Protection & Safeguarding Policy* will be followed, and this includes the recognition that it may be necessary to make external referrals for serious cases, to social services or the Police. Some forms of cyberbullying may entail criminal offences, such as upskirting or sharing child involved nudes / semi-nudes.

6.3 Search for/of electronic devices: In response to an allegation of cyberbullying, or some other significant behavioural or safeguarding concern that involves electronic devices, certain staff are permitted to conduct a search for and of electronic devices. Any searches will be conducted in accordance with the *Searches and Confiscation Policy*.

Searches take place where there is reasonable suspicion that an electronic device may be used to commit an offence, or cause personal injury (including the emotional harm of bullying) or damage to property. Parental consent is not required, but they will be informed after the event unless doing so presents a further risk to any child.

The School may also erase any data or files from the device if the School considers there to be good reason to do so, unless there are reasonable grounds to suspect that the device may contain evidence in relation to a criminal offence, where the files should not be deleted and the device must be given to the Police without delay.

If, following a search, the member of staff determines that the device does not contain any evidence in relation to a criminal offence, or are advised by the Police following a report to them that they will not take any further action to investigate an alleged offence, the School can decide whether it is appropriate to delete any files or data from the device, and may retain the device as evidence of a breach of this policy and the *Behaviour, Rewards and Sanctions Policy* (or any other relevant policy governing student conduct). The School may then take steps to sanction students, where appropriate. In the event that the search highlights a safeguarding concern in respect of any student, the School will follow the procedures set out in the *Child Protection & Safeguarding Policy*.

School staff can confiscate, retain or dispose of a student's property as a disciplinary penalty. The law protects staff from liability in any proceedings brought against them for any loss or damage to items they have confiscated, provided they acted lawfully. Staff will always consider whether confiscation is proportionate and consider any relevant special circumstances.

The School will keep a record of all searches carried out, including the results of any search, and the actions taken following that search.

6.4 Online harms and welfare considerations: Students may also be subject to risks and harms from online activities that are not related to or generated by other users at RBC. However, the School still has an important role to play in educating and protecting students from potential online harms and responding to incidents which arise. Proactive and reactive measures include:

- Training and education of students and staff, to identify a constantly evolving set of potential online harms, such as extremism, body image and health threats, promotion of self-harm, suicide, or other factors related to mental health, and new practices of grooming or exploitation.
- Open and timely communication with students and parents, and referral to additional sources of support both within the School and externally.

- Working as a pastoral team to ensure that there are 'eyes on' a child of concern, maximising information sharing, and considering a range of views – tutor, Head of Year, Director of Section, Medical, Chaplain, etc.
- Rapid referral to the DSL and effective management of safeguarding cases, with inter-agency working or liaison with other schools, bodies, as required.

The School also recognises the positive role that online communication can play in promoting good welfare and well-being, as a source of advice, affirmation, and emotional support. Staff (for example, tutors and tutor groups) are encouraged to have an open and on-going conversation with students about the constructive and destructive opportunities of online interaction. Listening without judgement and asking questions is an important part of this process, to better understand what students are doing and help identify risks.

6.5 Online safety and the Prevent Duty: Online safety and behaviours are an important consideration in the School's compliance with the *Prevent Duty Guidance* (2023). Online content is a significant risk factor in the radicalisation of individuals and informal communities, which could go on to harmful activities and – in worst cases – physical violence. The DSL is responsible for maintaining risk assessments to cover such concerns, which will include online risk. Furthermore:

- All staff are expected to be aware of the specific risk of online content as a tool for potential radicalisation and extremism. Staff must raise any concerns about online extremism or radicalisation as a safeguarding matter, following the *Child Protection & Safeguarding Policy*.
- Students are educated about the dangers of online radicalisation and extremism as part of the Wellbeing & Futures programme. Any participation in online extremism may well be interpreted as a behavioural, as well as a safeguarding concern.
- The Network Manager and DSL will ensure that appropriate filtering and monitoring helps to prevent the use of the School's network for radicalisation and extremism.

7. Digital Council Charter

A consultation of a student Digital Council in 2023 led to the formulation of a revised Charter, which reflects the views and concerns of students in terms of e-safety and online behaviour. The Charter is published to students in School documents and is as follows:

1. Everyone should treat people kindly and compassionately in just the same way in the online world as they would in the real world. It is important to focus on positive content online and use technology to support a positive atmosphere in the School.
2. Permission must always be given before using or uploading any information or media that involves another person.
3. Social media and communication groups should never be used as a medium for carrying out bullying or harassment. This includes deliberately excluding others, so they are left outside groups, as well as unwanted contact.
4. The School's systems should only be used for constructive and creative purposes. Systems like Teams chat or calls should not be abused or used in distracting, inappropriate ways.
5. Apart from in designated times and places for Sixth Form, phones should not be used or visible around School. This particularly applies in isolated areas where there is less visibility such as toilets.
6. Taking photos or videos of other people in the School community without their permission is not allowed.
7. Digital communication between all members of staff and students and their parents should only take place using the School email system and other designated systems, such as Teams. All members of the community should be understanding about response times and should not expect replies during the evening. Communication between students and staff via any private

social media platforms or personal email addresses is not allowed. Do not attempt to add or follow members of staff via social media.

8. Everyone must look out for others in the online world in the same way as in the real world. If they are concerned about themselves or someone else, they should report them to the School to ensure that everyone is safe. Ideally, members of our community should be 'active bystanders' online and challenge behaviours that are wrong.
9. Technology should be used in appropriate and fair ways for academic work. Artificial Intelligence should only be used to support academic work with the advice or suggestions given by members of staff. You should never copy-and-paste material from online and pretend it is your work. You should also make sure that technology does not distract you or prevent you from working.
10. Everyone must ensure that potentially addictive online activities (such as gaming) that are disruptive to well-being are kept in moderation, so they do not have an adverse impact on sleep, academic progress, and relationships with others.

8. Advice and resources

All members of the community are warmly invited to raise questions and concerns, and seek further advice from SLT. General advice and resources can be found below. Staff are encouraged to use and share this information with students.

8.1 Advice and resources for students: The following advice will help students to navigate their way through online life safely:

- Always respect others in what you say and do, and consider the impact of your actions online upon other people.
- Think before you send or share. What will this lead to? Will you have control of the situation? Who might see it? If in doubt – stop, then think again.
- Note the age-limits and advice for apps and services – stick to those limits and do not try to get around them. Think carefully about the safety implications that led to these age-limits in the first place.
- Guard your information and passwords. Do not share your passwords or secure information, make passwords are hard to guess, and change them regularly. If someone gets into your accounts, change your password and report immediately. Only give out your mobile number and other contact information to trusted friends.
- Block – bullies, inappropriate people, people you don't know or who make you feel uncomfortable. Most sites and services allow you to do this and to report.
- Do not retaliate or reply – cyberbullying is often intended to get a reaction and provoke.
- Save the evidence – make sure you know how to screenshot from your phone and other devices, and how to save evidence. Tell your teachers and parents that you have this evidence (although, make sure that you do not take screenshots of any nude or sexual images).
- Report and support – make sure that you make people aware and get support if you are hurt by anything online: your tutor and Head of Year, your parents, or call helplines such as Childline (0800 1111) or the NSPCC (0808 800 5000). Remember that nobody deserves to suffer or be harmed by anything online.
- Get guidance and help from recommended services:
    - https://cyberbullying.org/resources/students
    - https://www.childnet.com/young-people/
    - https://www.digitalawarenessuk.com/resources

8.2 Advice and resources for adults: The following advice is for parents and staff, to help them manage and respond to e-safety concerns about children:

- Have an open and on-going conversation with young people about safe and appropriate online activity.
- Assume that young people will have a stronger understanding of what goes on online than most adults – respect their knowledge and do not patronise.
- Set out ground rules that are clear and consistent, as early as possible. It is always easier to relax a strict rule with children later on than to impose a new, firmer rule when things 'get out of hand'. The best rules apply to all members of the household, so consider whether there are shared points that all could accept (e.g., no phones in bedrooms).
- Encourage young people to share their experiences of what they see online and do not be too quick to judgement – it is important to keep trust and not to close down channels of communication.
- Admit to your own mistakes and anxieties about life online; be human.
- If you become aware of a child being harmed or witnessing inappropriate behaviour online, be sure to help them access tools to respond to it – blocking, recording, reporting, and getting help from pastoral staff at School.
- Gain familiarity with the Online Safety Act (2023), which aims to protect children and young people from harmful and inappropriate content. See further:
    - https://learning.nspcc.org.uk/news/2023/november/what-online-safety-act-means-children-professionals
    - Online Safety Act: explainer - GOV.UK
- Get guidance and help from recommended services:
    - (Sites mentioned in student list above).
    - https://parentzone.org.uk/
    - https://www.ceop.police.uk/Safety-Centre/

9. Policy review and related policies

Review schedule:

Author(s):	Guy Williams (Deputy Head [Pastoral])
Date:	June 2026
Review Frequency:	Annually
Next Review Date:	June 2027
References:	• Teaching Online Safety in Schools (2023) • Meeting Digital and Technology Standards in Schools and Colleges (DfE, 2023) • Review of Sexual Abuse in Schools and Colleges (OFSTED, 2021) • The Prevent Duty Guidance (2023)
Associated Policies	• Anti-Bullying • Artificial Intelligence • Acceptable Use Policy (See Appendix 1) • Behaviour, Rewards and Sanctions • Searches and Confiscation • Child Protection and Safeguarding • Data Protection Policy • Staff Code of Conduct • Student Manual
Agreed by:	 Clare Freeman (Safeguarding Governor) *on behalf of the Full Governing Board*
Date of Agreement:	June 2026

Appendix 1: Acceptable Use Policy

Scope

This policy applies to all members of the School community (staff or students) who use school IT systems, as a condition of access. Access to school systems is not intended to confer any status of employment on any contractors.

Online behaviour

As a member of the School community you should follow these principles in all of your online activities:

- The School cannot guarantee the confidentiality of content created, shared and exchanged via school systems. Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the School community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the School community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the School's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the School's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the School's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the School monitors use of the School's IT systems, and that the School can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed, and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.
Passwords must adhere to the following criteria

- Minimum 8 characters
- An uppercase letter
- A lowercase letter
- A number or special character
- Cannot match a previous password

All staff accounts with access to student and/or sensitive data must be protected by Two Factor Authentication (2FA).

Use of Property

Any property belonging to the School should be treated with respect and care, and used only in accordance with any training and policies provided. You must report any faults or breakages without delay to the IT Services department.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and students should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the School's right to monitor and access web history and email use.

Use of personal devices or accounts and working remotely

All official school business of staff must be conducted on school systems, and it is not permissible to use personal email accounts for school business. Any use of personal devices for school purposes, and any removal of personal data or confidential information from school systems – by any means including email, printing, file transfer, cloud or (encrypted) memory stick – must be registered and approved by the IT Services department.
Where permission is given for use of personal devices, these must be subject to appropriate safeguards in line with the School's policies, including [two-factor authentication, encryption etc.]
Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any student nor to have any images, videos or other recording of any student on their personal devices. Please read this in conjunction with *Child Protection & Safeguarding Policy* and *Staff Code of Conduct*.

Monitoring and access

Staff, parents and students should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the School where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.
Any personal devices used by students, whether or not such devices are permitted, may be confiscated and examined under such circumstances. The School may require staff to conduct searches of their

personal accounts or devices if they were used for school business in contravention of this policy, and in particular if there is any reason to suspect illegal activity or any risk to the wellbeing of any person.

The use of Virtual Private Networks (VPNs), mobile hotspots and mobile data to circumvent the School's filtering and monitoring systems is expressly forbidden.

Tracking Devices and Technology

The School is not responsible for individual settings on personal devices, nor for the use of tracking apps/devices for purely personal and domestic purposes.

Use of this technology in the context of school activities is not specifically encouraged but if parents do plan to use it then they should be aware of potential third party privacy considerations and only use it for domestic/personal purposes in respect of their own child and/or their child's belongings.

Compliance with related school policies

To the extent they are applicable to you, you will ensure that you comply with the School's *E-Safety, Digital Communication and Student Device Policy*, *Child Protection & Safeguarding Policy*, *Anti-Bullying Policy*, *Data Protection Policy, GDPR Retention Policy, Privacy Notice* and the *Student Manual*.

Retention of digital data

Staff and students must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted. Email accounts will generally be closed and the contents archived within 1 month of that person leaving the School.

Student Account	Password changed within 7 days of leaving.	• Email/OneDrive backed-up and stored • Account deleted within 4 weeks
Staff Account	Password changed within 7 days of leaving.	• Email/OneDrive backed-up and stored • Account deleted within 4 weeks (unless longer access requested).

Any information from email folders that is necessary for the School to keep for longer, including personal information (e.g. for a reason set out in the School Privacy Notice), should be held on the relevant personnel or student file. Important records should not be kept in personal email folders, archives or inboxes, nor in local files. Hence it is the responsibility of each account user to ensure that information is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the School's email deletion protocol. If you consider that reasons exist for the protocol not to apply, or need assistance in how to retain and appropriately archive data, please contact Barry Hines, Head of IT Services (bjh@rbcs.org.uk).

Breach reporting

The law requires the School to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the School regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the School's systems, e.g. through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The School must generally report personal data breaches to the ICO without undue delay (i.e. within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the School must keep a record of any personal data breaches, regardless of whether they need to notify the ICO.
If either staff or students become aware of a suspected breach, they must report it immediately to the Data Protection Co-Ordinator (the Bursar).
Data breaches will happen to all organisations, but the School must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and students. The School's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Use of Artificial Intelligence

Any usage by students of generative AI tools such as Copilot is only permitted in the circumstances outlined in the *AI Policy*, where usage rules, protocols, etc are outlined, and subject to any conditions imposed by that policy. The key points are:

1. Copilot is the ***only*** generative AI tool authorised for use by students and staff at Reading Blue Coat. Students and staff are not permitted to use other generative AI tools, such as Google's Gemini and OpenAI's ChatGPT, without first seeking permission from the Designated Safeguarding Lead and IT Services & Support Manager.
2. ***Only*** students in Years 9-13 are permitted to used Copilot. Students in Years 7-8 are not permitted to use generative AI tools.

Personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, students should not use these tools to answer questions about health, medical or wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from the Designated Safeguarding Lead or IT Services & Support Manager.

Breaches of this policy

A deliberate breach of this policy by staff or students will be dealt with as a disciplinary matter using the School's usual applicable procedures. In addition, a deliberate breach by any person may result in the School restricting that person's access to school IT systems.
If you become aware of a breach of this policy or the *E-Safety, Digital Communications and Student Device Policy*, or you are concerned that a member of the School community is being harassed or harmed online you should report it to the Designated Safeguarding Lead. Reports will be treated in confidence wherever possible.

Appendix 2: Artificial Intelligence – Considerations and Actions for E-Safety

There is currently no specific guidance on A.I. for schools in the UK. However, the following appendix draws on various resources, such as:

AI in schools: What you need to know – The Education Hub
Guidance - AI Knowledge Hub - AI.GOV.UK
Guidance on AI and data protection | ICO
Generative AI: keeping learners safe online - Hwb
Responsible AI Toolkit - GOV.UK
Use of artificial intelligence in education delivery and assessment - POST

This appendix is not a comprehensive A.I. policy (see further the School's A.I. policy), but sets out the e-safety considerations and actions for engaging with A.I. at Reading Blue Coat.

Principles for engaging with A.I. safely

To engage with A.I. technologies safely and appropriately, members of the School community should adhere to the following principles:

- Assess the suitability of A.I. for a particular task and not use it indiscriminately.
- Comply with the law and Government guidance.
- Comply with relevant School policies (e.g., the *Acceptable Use Policy*).
- Only make use of A.I. in ways that are consistent with safety, wellbeing, and good conduct.
- Provide / access appropriate education, training, and information for all members of the School community: students, staff, parents, Governors.
- Ensure that the risks and benefits of A.I. are presented to students in a thorough, relevant, and balanced way.
- Ensure data security and data protection; do not enter sensitive or personal information into A.I. tools without specific guidance from the School's Data Protection Officer.
- Do not infringe copyright or other intellectual property conventions.
- Only use A.I. technologies that are approved by the School and age appropriate.
- Report all incidents promptly in accordance with relevant policies (e.g., abusive use of A.I. should be reported to the Designated Safeguarding Lead).
- Audit and risk assess the use of specific A.I. systems that are approved by the School.
- Be aware of risks of discrimination and bias in A.I. outputs, and the potential to distort reality and mislead.
- Ensure transparency in A.I. generated content, so that anything produced in this way is labelled as such.
- Critically evaluate the use of A.I. in any decision making process and ensure that humans are still clearly the decision makers, with their own rationales.
- Ensure that abuse and misuse is tackled robustly through existing School policies.

Areas of responsibility

The Governors are responsible for understanding how A.I. is used at RBC and ensuring that appropriate measures are put in place to support safe and appropriate use.

The Headmaster and Senior Leadership Team are responsible for deciding the strategy for the use of A.I., including the identification of specific tools and systems that are approved or prohibited.

The Deputy Head (Education Development) is responsible for guiding staff to implement appropriate use of A.I. in the classroom and in homework.

The Deputy Head (Pastoral), who is also the Designated Safeguarding Lead, is responsible for promoting safe use of A.I., and for responding to harmful or abusive use. They are also responsible for any behavioural and disciplinary issues in relation to A.I.

The Data Protection Officer, who is also the Bursar, will provide any guidance necessary for data protection issues in relation to A.I., and will lead any response to data breaches as per the *Data Protection Policy*.

All teaching staff are responsible for guiding students in safe and appropriate use of A.I. in their academic endeavours.

All members of the School community are expected to following the principles set out here and to adhere to other relevant policies.

Reporting issues

Issues involving the use of A.I. should be reported as per the requirements of relevant policies: safeguarding concerns to the Designated Safeguarding Lead, staff allegations to the Headmaster, etc. If a member of staff is in doubt as to whom an issue should be reported, they can take advice from the Deputy Head (Pastoral) / Designated Safeguarding Lead.

As with any other issues, students should report their concerns to their Tutor in the first instance.

Specific A.I. e-safety risks

In promoting a positive culture of e-safety, it is important for all staff to stay up-to-date with new and emerging risks, particularly those that occur through rapidly advancing A.I. technologies. A non-exhaustive lists of risks to be aware of includes:

Deepfake technologies – using A.I. to produce realistic but fake media, including images and videos. Deepfakes could be used for a variety of harmful, illegal, or abusive purposes such as creating sexual imagery without consent or promoting political misinformation.

Exposure to illegal content – the products of A.I. may be illegal, with the use of A.I. to generate child sexual abuse material being a particular concern. Such content is extremely harmful and illegal, even if it is not 'real'.

Peer harassment and abuse – fake media generated through A.I. could be used to harass and abuse through online communication and social media. Such abuse could be sexual in nature, generating media from other images and video. It could be intended to humiliate. It could involve text or sound as well. Some media could be 'pseudo-media' that is deliberately cartoonish or unrealistic; it is important to note that this may be just as harmful and illegal.

Spread of harmful misinformation – A.I. generating technologies could be used to create convincing fake media that can spread harmful ideas – conspiracy theories, extremist views, and false reporting of current affairs and politics. Such content could foster harmful and dangerous attitudes and behaviours among impressionable young people.

Online scams – A.I. generated chatbots, messages, and fake profiles could be used to target individuals to hand over personal information or trick them into handing over money.

Chatbots – some A.I. chatbots are potentially harmful. They may be used as an unhealthy substitute for social interaction. They may also engage in sexually explicit conversations and media, which may be age-inappropriate and/or put users at risk.

Training

All staff receive training about e-safety and A.I. as part of the rolling programme of annual safeguarding training.

All teaching staff receive training on safe and effective use of A.I. for academic purposes.