HONESTE VIVERE

CAXTON COLLEGE

SINCE 1987

Whole School Technology Policy

2023-2024

Review Date: August 2024
Responsible: AHT´s responsible for Technology(Primary and Secondary)

Review Date: August 2024
Responsible: AHT´s responsible for Technology (Primary and Secondary)

Caxton College recognises that ICT and the Internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. All staff and pupils from years 5 to 13 have an iPad to support and enhance their learning, supported by a powerful infrastructure including Wifi coverage across the school and Apple TV in every classroom. The school is eager for pupils to make the most of the opportunities afforded by the use of technology, but does so with the safeguarding of every child's welfare at the heart of every decision. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good online use. It is important that all members of the school community are aware of the dangers of using the Internet and how they should conduct themselves online.

One of the core principles of this Technology Policy is online safety that covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. A "duty of care" exists for individuals engaged in the supervision of children, and the imperative of instructing all members of the school community about the perils and obligations related to online safety is encompassed within this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. Online safety is a whole-school issue and responsibility.

This policy should be read in conjunction with the following policies:

- Safeguarding and Child Protection
- Anti-Bullying
- Wellbeing
- Behaviour for Learning
- Literacy
- Data Protection/GDPR
- Staff Acceptable Use Policy (Appendix A)
- Student Acceptable Use Policy (Appendix B)
- Primary E-safety and iPad rules (Appendix C)
- Secondary 5 essential technology rules, e-safety guidelines, BYOD Policy(Appendix D)
- Remote Working Policy (Appendix E)

1. Roles and Responsibilities

Headteachers and Leadership Teams
They are responsible for the approval of the Technology policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Headteachers have a duty of care for ensuring the safety (including online safety) of all members of the school community, though the day-to-day responsibility for online safety will be delegated to the Assistant Head of Technology. Any complaint about staff misuse must be referred to the Assistant Head of Technology at the school or Head Teacher.

Their roles will ensure:

- A Technology policy is in place, reviewed every year and/or in response to an incident.
- There is an Technical online safety coordinator (Assistant Head of Technology) who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive.
- Procedures for the safe use of ICT and the Internet are in place and adhered to.
- All members of staff are accountable for online safety.
- Access to induction and training in online safety practices for all users.
- All staff receive regular, up to date training.
- Appropriate action is taken in all cases of misuse.
- Internet filtering methods are appropriate, effective and reasonable.
- Staff or external providers who operate monitoring procedures are supervised by a named member of SLT/PLT.
- Pupil or staff personal data as recorded within the school management system sent over the Internet is secured.
- The school ICT system is reviewed regularly regarding security and that virus protection is installed and updated regularly.

Assistant Heads of Technology:

- Lead online safety meetings with Safeguarding committee and staff training.
- Work in partnership with the school ICT Managers to ensure systems to protect students are reviewed and improved.
- Ensure the school ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Review reports of online safety incidents to inform future online safety developments.
- Report to the Leadership Team.

ICT Managers / Technical Staff:

The ICT Manager is responsible for ensuring that:

- The school's technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets required online safety technical requirements and any relevant body Technology policy / guidance that may apply.
- Users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant.
- The use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher; Assistant Head of Technology for investigation / action / sanction
- Monitoring software / systems are implemented and updated as agreed in school policies.

2. Communicating School Policy

This policy is available for parents, staff and pupils. Parents can access it on their parent profile under the documentation section and available to staff and students via google drive.

3. Making use of ICT and the Internet in school

The internet is an essential element in 21st century life for education, business and social interaction. We want to equip our students with all the necessary ICT skills that they will need to enable them to progress confidently into a professional working environment when they leave school.
The school has a duty to provide pupils with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. As well as affording excellent research opportunities, it also enables the sharing and review of work, flipped learning opportunities, innovative ways of submitting and of marking work , as well as disseminating notes and information. Beyond this, and perhaps more importantly, the routine use of iPads and technology prepares pupils for a world which is increasingly dependent on digital technologies. The Internet is used in the school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
The school internet access is provided by Vodafone and as a backup system Quattre. Our filtering system is appropriate to the age of pupils: the providers are Fortinet for desktop and laptop computers and IMT Lazarus in conjunction with Jamf School for iPads. SonicWall filters content such as pornography, gambling, hacking, malware, terrorist and extremist material and social media sites. Jamf School limits and ensures that the applications available during the school day on the student's ipads are only those which have been predetermined by the school.
Pupils are taught what internet use is acceptable and what is not and are given clear objectives for internet use; they are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. They are shown how to publish and present information appropriately to a wider audience and are taught how to evaluate internet content and how to validate information before accepting its accuracy. Above all the School endeavours to ensure that pupils are critically aware of the materials they read. The school always seeks to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.

Some of the benefits of using ICT and the Internet in schools are:

For pupils:

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Opportunities for contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for pupils to interact with people that they otherwise would never be able to meet.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.
- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Improved access to technical support.
- Ability to provide immediate feedback to students and parents.

- Class management, attendance records, schedule, and assignment tracking.

4. Learning to Evaluate Internet Content

With so much information available online it is important that pupils learn how to evaluate Internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught to:

- Be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- Use age-appropriate tools to search for information online
- Acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously. Students who are found to have plagiarised will be disciplined.

The school will also take steps to filter Internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites, then the URL will be reported to the ICT Managers. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

As a part of the micro CPD sessions, staff have the opportunity to share good practice, tools for learning and receive training.

5. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The ICT Managers will review the security of the school information systems and users regularly and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet is encrypted.
- Files held on the school network will be regularly checked for viruses
- The use of user logins and passwords to access the school network will be enforced

For more information on data protection in school please refer to our **data protection policy**. More information on protecting personal data can be found in **section 12** of this policy.

6. Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication.

Staff and pupils should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. Pupils must not reveal personal details of themselves or others in an email communication, or arrange to meet anyone without specific permission. Pupils must immediately tell a teacher if they receive an offensive email.

The school has the right to monitor emails and their contents *but will only do so if it feels there is reason to.*

6.1 School Email Accounts and Appropriate Use

Students through year 5 to year 13 have Google apps accounts. All these accounts are managed and monitored by the ICT managers to ensure their safe usage. Pupils from year 5 to 13 are identifiable using their school email account; internally this allows teachers to interact with their classes via online learning platforms and track pupils progress, etc. However external communication is not permitted for students from year 5 to year 10. and sharing of files to non approved sources is not permitted from years 5 to 13 outside of the school domain.

Staff should be aware of the following when using email in school:

- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
- Emails sent from school accounts should be professionally and carefully written. Staff are always representing the school and should take this into account when entering into any email communications.
- Staff must tell their ICT Managers or a member of the leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- Staff is trained to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Students should be aware of the following when using email in school, and will be taught to follow these guidelines:

- In school, pupils should only use school-approved email accounts
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails. They should not attempt to deal with this themselves.
- Pupils must be careful not to reveal any personal information over email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge.
- Pupils will be educated annually to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

Parents should be aware of the following when using email to contact the school

- Parents can communicate with the school via the schools parent profile or via direct email to a teachers school account.

7. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published. The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information are not published.

The Director of Communication takes overall editorial responsibility and ensures that the content on the school website,all the publications and press releases are accurate and appropriate.

7.1 Policy and Guidance of Safe Use of Children's Photographs and Work

Photographs and pupils' work bring our school to life, showcase our student's talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the General Data Protection Regulation images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. For students aged 14 and above their consent is also required.

7.1.1 Using photographs of individual children

Published images do not identify students or put them at risk of being identified. Only images created by or for the school will be used in public and children may not be approached or photographed while at school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children.

- Parents and others attending school events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The school does not prohibit this as a matter of policy.

- The school does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the school to prevent.

- The *school* asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.

- As a school we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.

- Whenever a pupil begins their attendance at the school they, or their parents where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. We will not use images or videos of pupils for any purpose where we do not have consent.

7.2 Complaints of Misuse of Photographs or Video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our **complaints policy** for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools **child protection and safeguarding** policy and **behaviour policy.**

Our pupils increasingly use electronic equipment daily to access the internet and share content and images via social networking sites. Unfortunately, some adults and young people will use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to grooming and enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings.
Pupils may also be distressed or harmed by accessing inappropriate websites that promote unhealthy lifestyles, extremist behaviour and criminal activity.

Misuse of photographs or videos in any form will be dealt with in accordance with the school Behaviour Policy according to the incident type.

7.3 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. The school has a variety of activities and whole school events including Safer Internet Day, competitions, the RSE curriculum, visits and talks from Guardia Civil.
- Any sites that are to be used in class should be evaluated by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run from the school website with the approval of a member of staff and will be moderated by a member of staff.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are always representing the school and must act appropriately.
- Safe and professional behaviour of staff online will be discussed in staff CPD.

8. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Staff are expected to lead by example and be good technology role models. Some of the measures are outlined below:

- Primary students are not allowed to bring mobile phones to school.
- KS3 and KS4 students are not allowed to use mobile phones at any point during the school day (from 09.00 - 16.30). If KS3/4 pupils are seen in possession of a mobile phone during school hours, the device will be confiscated and kept in the school safe where parents will then be required to collect it.
- KS5 students can bring mobile phones to school, but they cannot use them inside the buildings, or in Primary or Secondary Playgrounds.
- KS5 students can only use mobile phones inside the Sixth Form Common Rooms and in the designated areas outside the Common Rooms that are clearly marked.
- Headphones can only be used in designated areas – these are the Library, 6th Form Common Rooms, and classrooms (when specifically given permission by teachers)
- Under no circumstances can pupils take photos or videos on their mobile devices
- Under no circumstances are pupils allowed to bring mobile phones or personal devices into examination rooms with them.
- A member of staff can confiscate mobile phones, and a member of the senior leadership team can search the device if there is reason to believe that there may

be evidence of harmful or inappropriate use on the device.

- Any pupil who brings a mobile phone into school is agreeing that they are responsible for its safety. The school will not take responsibility for personal devices that have been lost, stolen, or damaged.
- The school will not tolerate cyber bullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined.

8.1 Mobile Phone or Personal Device Misuse

Pupils

- Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school's behaviour policy. Their mobile phone may be confiscated.
- Pupils are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a pupil is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the pupil being prohibited from taking that exam.

Staff

- Staff should not use their own personal mobile or email to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils with their personal mobiles. The school equipment will be used for this.
- Mobiles may be used by staff in the staff rooms, offices and in the entrance to primary, the main reception, or any other waiting zones of the buildings or classrooms when no pupils are present.
- The use of mobile phones by staff is not permitted in classrooms when pupils are present or in the dining rooms, corridors, playgrounds except for the staff who need it for their responsibilities as playground supervisors.
- Staff can use their mobile at any time if they need to communicate a medical emergency to the school nurse.
- Where staff may need to take a call of a more sensitive nature (personal, medical etc.), they may use an outdoor space only when they can ensure they are not in the presence of pupils. Staff should not use their mobile phones outside at break time or lunchtime or at any time in front of pupils
- Any breach of school policy may result in disciplinary action against that member of staff.

Visitors

- All visitors are shown the safeguarding guide, which includes mobile phone use regulations (see Appendix F)

9. Online Safety Rules

At Caxton College we want students to use technology and the Internet to help them to learn.
All Staff are trained that the following online safety rules alongside the documentation given to students are a key part in teaching the students on how to conduct themselves online.
All the adults working with students will help to keep them safe but there can be some risks, so we urge students to behave responsibly at all times and follow these rules:

- I will only use IT systems in school, including the internet, email, digital video, iPad, etc. for school purposes.
- I will not use IT systems at school for personal financial gain, gambling, political activity, advertising or illegal purposes.
- I will only log on to the school network, wifi or learning platforms with my own username and password.
- I accept that I am responsible for all activity carried out under my username.

- I will follow the school’s IT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school email address for school-related work, and where appropriate
- I will make sure that all IT communications with pupils, teachers or others are responsible and sensible, particularly as emails could be forwarded to unintended readers.
- I will be responsible for my behaviour when using any online or digital services. This includes resources I access and the language I use.
- I will not look at websites which are not part of the lesson.
- I will be polite and appreciate that other users might have different views to my own.
- I will not give out any personal information such as name, phone number or address through email, personal publishing, blogs, messaging or when using any of the online services you have signed up to.
- I will use nicknames and avatars online to keep my personal information safe.
- I will not arrange to meet someone I have met online unless this is part of a school project approved by my teacher.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not download or install software on school technologies.
- I will not attempt to bypass the internet filtering system or device management service.
- I will only download or upload files with my teacher´s permission.
- I will only open/delete my own files.
- I will not open an attachment unless I know who sent it.
- I will not use any social networking sites or chat sites /apps in school.
- I will only use a camera or video in school or on a trip with my teacher´s permission.
- I will never use a camera or video in the playground, clubs, birthday parties or on the school bus.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will respect the privacy and ownership of others’ work on-line at all times.
- I understand the school can exercise its right to monitor the use of the school’s computer systems and learning platform, including access to web-sites, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school’s computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
- I understand that all my use of the internet, the school's learning platform and other related technologies can therefore be monitored and logged and can be made available to my teachers.
- I will always ask an adult if I am unsure of anything when I am online.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents/carer may be contacted.
- I understand that bullying of any kind through the internet, computers or mobile devices will not be tolerated. I will tell an adult if I think it's happening to me or others.
- Year 5 & 6 have a general ‘Help’ button on their iPad to report anything upsetting that they see when online. This information is sent directly to the Assistant Headteacher.
- Pupils in Secondary are taught to report bullying incidents online by using the Stopbullying icon on their ipads or StopBullying email address. This information is sent directly to the Assistant Headteacher and the relevant Head of Year.

Primary (Y5 & 6) has a child-friendly version of the online safety rules and iPad rules that are shared with children and added to the parent profile. See appendix C

Secondary (Y7 to 11) students are all given access to pupil e-safety guidelines and iPad rules (5 essential technology rules) that are located on their ipads. See appendix C

Year 12 to Year 13 students that choose to bring a laptop are given a BYOD User Agreement outlining the online safety rules of the school. These rules are in addition to the ones above and are specifically designed to encourage them to be responsible with their personal device. See appendix D

10. Cyberbullying

The school, as with any other form of bullying, takes Cyber bullying very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **behaviour policy and/or the school anti-bullying policy.** The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider to identify the bully
- Record and report the incident, if it is a potential safeguarding issue then a report should be recorded on the MyConcern platform
- Provide support and reassurance to the victim
- Make it clear to the ‘bully’ that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.
- Repeated bullying may result in fixed-term exclusion.

If a sanction is used, it will correlate to the seriousness of the incident and the ‘bully’ will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

11. Managing Emerging Technologies

Technology is progressing rapidly, and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

12. Protecting Personal Data

Caxton College believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect, and process is used correctly and only as is necessary, and the school will keep parents fully informed of how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the General Data Protection Regulation, and following principles of good practice when processing data, the school will:

- Ensure that data is fairly and lawfully processed
- Process data only for limited purposes
- Ensure that all data processed is adequate, relevant and not excessive
- Ensure that data processed is accurate
- Not keep data when permissions are revoked
- Process the data in accordance with the data subject's rights
- Ensure that data is secure
- Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external organisations. These organisations are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school's safeguards relating to data protection **read the school's data protection policy** which can be found on the school website and on the school drive.

This policy will be reviewed annually

APPENDIX A

IT Acceptable Use Policy for Staff

IT and related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to adhere at all times to its contents. Any concerns or clarification should be discussed with the Primary Headteacher or Secondary Co-Heads.

As a member of staff, trustee or visitor to the school, you are required to adhere to the following statements:

- I appreciate that IT includes a wide range of systems, including my iPad, mobile phones, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.
- I understand that it may be a criminal offence to use a school IT system for a purpose not permitted by its owner.
- I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the school's email, internet, learning platforms and any related technologies for professional purposes.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Hard copies of sensitive personal data should only be taken out of school when authorised . Sensitive personal data should not be transferred to external hard drives, including USB sticks.
- When working away from the school site, I will refer to the guidelines given in the Remote Working policy. (Appendix E)
- I understand the importance of protecting and monitoring my use of data in line with GDPR regulations.
- I will not install any hardware or software without the permission of the Primary Headteacher or Secondary Co-Head.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that my use of the internet and email, when accessed through the School network can be monitored.
- I will respect copyright and intellectual property rights.
- Images and audio recordings of pupils and/or staff will only be taken, stored and used for professional purposes in line with school policy and (where appropriate) with written consent of the parent, carer or staff member. Images and audio recordings will not be distributed outside the school network/learning platform without the permission of the parent/carer.
- I will ensure that my online activity will not bring the School into disrepute.
- I will strive to ensure that all electronic communications with parents, pupils and staff, including email and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school´s Technology Policy and help pupils to be safe and responsible in

their use of IT and related technologies. I will promote online safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the Safeguarding Team, Primary Headteacher or Secondary Co-Head (Pastoral).
- I understand that sanctions for disregarding any of the above will be in line with the School's disciplinary procedures and serious infringements may be referred to the police.
- I understand that this policy will be updated regularly, in line with policy changes within or outside of school and that it is my responsibility to read new versions of this document.

APPENDIX B

IT Acceptable Use Policy for Students (Year 7 to 13 Ipad Users)

Every time you use technology or connect to the internet you need to be aware of the possibilities that are available to you, how to behave responsibly and how to stay safe. It is important that your actions show respect to anyone that could see your presence online, whether they are directly known to you or not. Equally you must ensure that you limit your audience only to those that you want to view your content wherever possible. Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

The following statements form the Pupil Acceptable Use Policy:

- I understand it is against school rules to use a computer or network for a purpose not permitted by the school.
- I will choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships.
- I will not be obscene either in the words that I use or the content that I view. This includes material that is violent, racist, sexist or adult in nature.
- I will also respect the laws of copyright and ensure that the sources used are referenced.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details.
- I will not take or distribute any images or videos of people without the consent of my teacher.
- I will never use my device to bully or upset anyone and will report any instances of bullying that I come across.
- I will use my device as directed by my teachers and will do nothing to bring the school into disrepute.
- I will only use my school email address for school-related work, and where appropriate.
- I will not attempt to circumvent the school's filtering or device management service in any way.
- I will only be connected to the 'Caxton1to1' network.
- I will not have any other devices connected to the network.
- I will only ever use my own account.
- I will not attempt to modify static IT equipment.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted.
- Social media may only be used at the discretion of my teacher.
- I will not arrange to meet someone I have met online.
- Profiles created for school-based accounts will use the anonymized (numerical) emails given to me. I will not use real photographs of myself as an avatar, and where possible I will give reduced personal information such as my first name and first initial of my surname. I should speak to a member of staff about creating these accounts if I am unsure.
- The playing of games is not permitted whilst on the school site.
- I will remain signed in to my school security profile on the ipad at all times.
- I will acknowledge and adhere to the "eSafety Guidelines" posted on my ipad
- I have read and understood the school's behaviour policy for device misuse.

IT Acceptable Use Policy for 6th Form

Your use of technology and the internet should show an awareness and respect for both yourself and others. Every time you use technology or connect to the internet you need to be aware of the possibilities that are available to you, how to behave responsibly and how to stay safe. It is important that your actions show respect to anyone that could see your presence online, whether they are directly known to you or not. Equally you must ensure that you limit your audience only to those that you want to view your content wherever possible. Your online presence (digital footprint) should be a positive one, as should your use of technology in school.

The following statements form the Pupil Responsible Use Policy (6th Form BYOD Version):

- I understand that the only permissible devices for use in the classroom are an iPad or for laptops, the school accepts Mac (Apple) and Windows operating system. Devices with a Linux operating system will not be accepted.
- I will ensure that the device I am using for school purposes is signed into Caxton Students Wifi network and has my school email account setup on it at all times.
- I understand it is against school rules to use a computer or network for a purpose not permitted by the school.
- I will choose usernames that are appropriate and consider carefully what personal information I give out about my life, experiences and relationships.
- I will not be obscene either in the words that I use or the content that I view. This includes material that is violent, racist, sexist or adult in nature.
- I will also respect the laws of copyright and ensure that the sources used are referenced.
- I will not share content that puts me, or anyone else at risk in any way, this includes revealing passwords, personal details, photos or my location and will tell an adult should someone ask me for these details.
- I will not take or distribute any images or videos of people without the consent of my teacher.
- I will never use my device to bully or upset anyone and will report any instances of bullying that I come across.
- I will use my device as directed by my teachers and will do nothing to bring the school into disrepute.
- I will only use my school email address for school-related work, and where appropriate.
- I will not attempt to circumvent the school's filtering or device management service in any way .
- I will only ever use my own account
- I will not attempt to modify static IT equipment.
- I understand that torrenting, peer to peer networks or illegal file sharing are not permitted
- Social media may only be used at the discretion of my teacher
- I will not arrange to meet someone I have met online
- Profiles created for school-based accounts will use the anonymized (numerical) emails given to me. I will not use real photographs of myself as an avatar, and where possible I will give reduced personal information such as my first name and first initial of my surname. I should speak to a member of staff about creating these accounts if I am unsure.
- I have read and understood the school's behaviour policy for device misuse.
- I have read the document and signed the 'BYOD agreement ' and agree to follow its guidance. I will follow these guidelines during the school hours for as long as the device is being brought into the school environment.

BYOD Bring Your Own Device (BYOD) is only available to those in the Sixth Form. Pupils in the Sixth Form are expected to have read and follow the BYOD version of the Pupil Acceptable Use Policy. Any questions about this should be raised with your tutor or Head of Year who will pass them on to the relevant member of staff. Mobile Phones may be used by Sixth Form pupils, but only in the Sixth Form Common rooms and designated spaces . They may not be used for sending messages or making phone calls during lesson time.

Appendix C

Primary

E Safety and iPad Rules

At Caxton College we want you to use technology and the Internet to help you to learn. All the adults working with you will help to keep you safe but there can be some risks, so we need you to behave responsibly at all times and follow these rules:

* I will use ICT in school **for school work**, with the **permission of my teacher**.

* I will keep my **passwords safe and private**.

* I will always **ask an adult** if I'm unsure of anything when I'm online.

* I will **not look at websites** which are not part of the lesson.

* I will **use nicknames and avatars** online to keep my personal information safe.

* I will **not share personal details** about myself or others, such as my full name, address or telephone number, and must not arrange meetings with anyone I meet online .

* I will **not open an attachment** unless I know who sent it.

* I will only **download or upload** files with my teacher's permission.

* I will only **open/delete my own files**.

* I will not use **any social networking sites** or chat sites/apps in school.

* I will make sure that all ICT contact with other children and adults is **responsible, polite and sensible.**

* I understand that **bullying of any kind** through the internet, computers or mobile devices will not be tolerated. I will tell an adult if I think it is happening to me or others.

* I will only use a **camera or video** in school or on a trip **with my teacher's permission.**

* I will **never use a camera or video** in the playground, clubs, birthday parties or on the school bus.

* I will **follow the iPad rules** at all times.

* I know that my use of ICT **can be checked** and that my parents will be contacted if a member of school staff is concerned about my e-Safety.

* I know how to use technology and the Internet **responsibly** and will keep to these rules.

* I will not look for nor bypass the school filtering or device management service.

* I will not post photos or videos of myself, or other pupils, when wearing school uniform on social media or messaging services.

Be Safe and...

… keep my iPad in my bag coming to and from school and take it out when I arrive at class.

… keep my iPad in a safe place and never leave it unattended

… ensure my iPad always has a protective cover on and carry it with two hands.

… keep food or drinks away from my iPad since they may cause damage to the device.

… store my iPad in the designated area if I am attending clubs or a birthday party after school.

Be Responsible and...

… only use apps and web pages that my teacher has given me permission to use.

… bring my iPad fully charged to school each day.

… not change the settings wallpaper (which should be a photo of myself) or remove the profile.

… ask my teacher if I have a problem and understand that my iPad may be checked at any time without notice.

Be Respectful and...

… stay on task.

… sleep my iPad when my teacher is talking to the whole class.

… only use the camera or microphone when my teachers tells me too.

… only use the iPad in the classroom under the supervision of my teacher.

... keep it in my bag on the bus/ in car room and not use it on the playground during playtimes.

...always ask for permission before I video or photograph someone.

… follow the school’s e-safety rules.

Appendix D

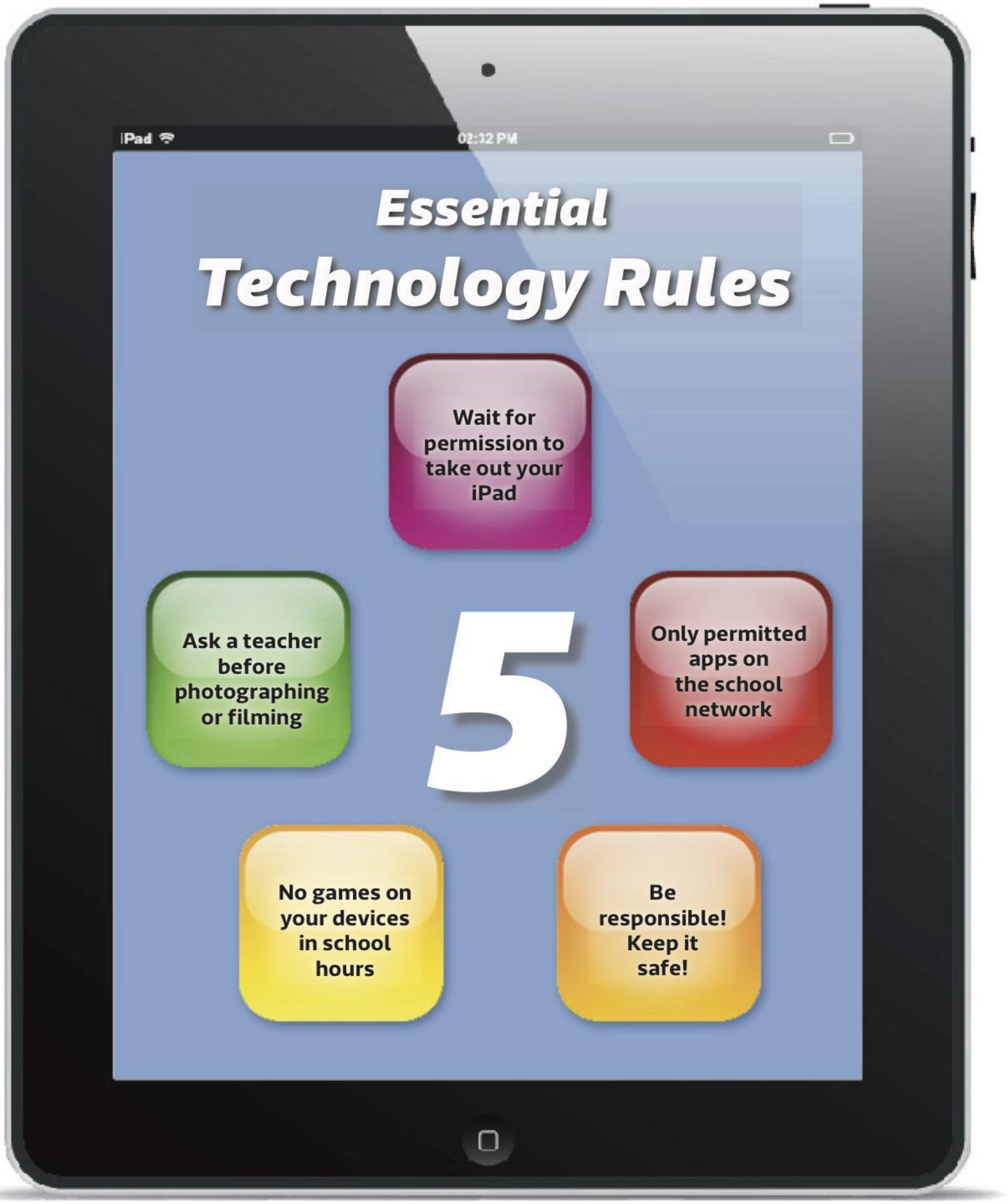
Secondary

E Safety Guidelines

At Caxton College we want you to use technology and the Internet to help you to learn. All the adults working with you will help to keep you safe but there can be some risks, so we need you to behave responsibly at all times and follow these rules:

- I will store my iPad in my locker during breaks to keep it safe.
- I will keep my passwords safe and private.
- I will always ask an adult if I'm unsure of anything when I'm online.
- I will not look at websites which are not part of the lesson.
- I will use nicknames and avatars online to keep my personal information safe.
- I will not share personal details about myself or others, such as my full name, address or telephone number, and must not arrange meetings with anyone I meet online .
- I will not open an attachment unless I know who sent it.
- I will only download or upload files with my teacher's permission.
- I will only open/delete my own files.
- I will not use any social networking sites or chat sites/apps in school.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I understand that bullying of any kind through the internet, computers or mobile devices will not be tolerated. I will tell an adult if I think it is happening to me or others.
- I will only use a camera or video in school or on a trip with my teacher's permission.
- I will never use a camera or video in the playground, clubs, birthday parties or on the school bus.
- I will follow the iPad rules at all times.
- I know that my use of ICT can be checked and that my parents will be contacted if a member of school is concerned about my e-Safety.
- I know how to use technology and the Internet responsibly and will keep to these rules.
- I will not look for nor bypass the school filtering or device management service.

CAXTON COLLEGE



Essential 5 Technology Rules

Wait for permission to take out your iPad

Ask a teacher before photographing or filming

Only permitted apps on the school network

No games on your devices in school hours

Be responsible! Keep it safe!

CAXTON COLLEGE

BRITISH SCHOOL SINCE 1987

CAXTON COLLEGE

BRING YOUR OWN DEVICE (BYOD) POLICY

This policy and agreement form has been devised to allow a restricted number of personal devices to be used in school and allow for an even greater level of individualised learning. The Sixth Form students who request and are granted access to the school's network via their own devices are expected to use their personal device within the rules outlined in this policy. They should read, and recognise that they are bound by the rules and requirements set out in this policy and the pupils e-Safety Agreement (located in the student's diary)

Student Guidelines

1. The primary purpose of the use of a personal device at school is educational.

2. The use of a personal device during lessons is at the discretion of teachers or staff.

3. Students must make no attempt to circumvent the school's network security or internet filtering; this includes, but is not limited to setting up proxies or using programs to try to bypass security.

4. Students must not upload/distribute pictures or video or any other material relating to students or staff without their permission. This includes, but is not limited to, emailing/snapchatting/messaging an image or video to posting an image or video on a social networking site.

5. Personal devices must not disrupt the class, others or study areas in any way.

6. Students are responsible for:

    - Ensuring their personal device is free from viruses and unsuitable material before bringing the device into school.

    - The safety of their device and **no** secure facility will be provided to store their personal device at school. **Students must keep their personal device with them at all times.**

    - Ensuring the device is functionally operational (charged and available for use in any lesson)

    - The use and the misuse of their registered devices.

    - The maintenance, protection and security of their device.

7. The school is entitled to confiscate any device should an investigation need to be carried and due to serious misuse of the device.

8. Students agree that the school can check their ipad and/or laptop including which sites they have visited while connected to the school network.

Caxton College is in no way responsible for:

- Any personal device that is broken whilst at school or during school-led activities.

- Any personal device that is lost or stolen at school or during school-led activities.

- The maintenance or upkeep of any device (charging, updating or upgrading, fixing software or hardware issues).

- The insurance of any device brought into school. This is the sole responsibility of parents/guardians and must provide adequate cover for the cost of repair/replacement or, in the respect of loss/theft of the device.

Sanctions

In addition to the sanctions stated in the school's Behaviour Policy, one or more of the following sanctions may apply:

- The privilege of using a personal device in school will be removed.
- A breach of the law may lead to the involvement of the police.

Appendix E

Remote Working Policy

Remote access via Google apps and working digitally from home are a normal and accepted part of working at Caxton College. There are a number of ways in which staff access and create content for work purposes and these guidelines aim to give clear parameters as to how data should be accessed and processed when not on site. All users should be aware of their own responsibilities when accessing data remotely and working off site; these responsibilities are primarily around confidentiality and data protection.

User responsibilities and good working practices

- Understand and adhere to contractual, ethical or other requirements attached to the information and in line with the school policies and procedures.
- To know what information they are accessing, using or transferring.
- Users are responsible for following correct procedures when logging out of the school accounts..
- 3rd party devices should not be considered or assumed to be secure and the use of such devices for storing documents or other work related to the school is discouraged.
- Appropriate precautions and good practice should be followed for all data and information that has been edited, created and/or saved on mobile or home devices.
- If users are using their own personal systems or other mobile devices to carry out work for the school then the following points should be followed:
    - Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner
    - Maintain safe web-surfing practice.
    - Each device should be kept up to date with anti-virus software
    - Maintain good practice with use and storage of passwords
    - Do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that are not relevant to your role.
    - Mobile devices are not left unattended
    - Data that is deemed confidential is not left visible on screens in public areas
    - If a system has suffered loss of data, corruption of data or any other issues that may impact the network or other systems at Caxton College, this is reported as soon as possible to the IT managers.
- The use of a school-provided iPad or other device provided by the school is considered secure for remote access as long as the following additional guidelines have been enacted:
    - Stay up to date with current security threats and issues for their device type, whether that is related to hardware or software, and update software appropriately and in a timely manner.
    - The iPad has a passcode and the 'lock screen automatically' function is enabled
    - Return the device to IT Support if you encounter any system faults or any other security related issues
    - Maintain safe web-surfing practice.
    - Passwords are kept private and not made available to other users
    - iPads or other devices are not left unattended
    - Data that is deemed confidential is not left visible on screens in public areas
    - Do not respond to unsolicited emails or click any link within unsolicited emails, pop-ups and other means of communication that is not relevant to your role.

Creating and processing data remotely

- Data created remotely in connection to work should not be shared in any way other than through Caxton College authorised platforms, namely: Google Drive, Google Classroom. Users should carefully consider which platform to use when sharing content remotely.
- Sensitive data should only be transmitted if necessary internally using the school portal or using school email accounts.

Remote Access for Third Party Suppliers

It is often necessary for third party suppliers to require remote access to install, upgrade or troubleshoot the school systems. In these instances remote access should be monitored until the completion of the installation and the remote session has ended. Third party suppliers remotely accessing Caxton College systems must contact the school and inform them of any changes that are to be made along with times and dates of the required remote access session.

User accounts for third party suppliers and support should be kept disabled when not in use.

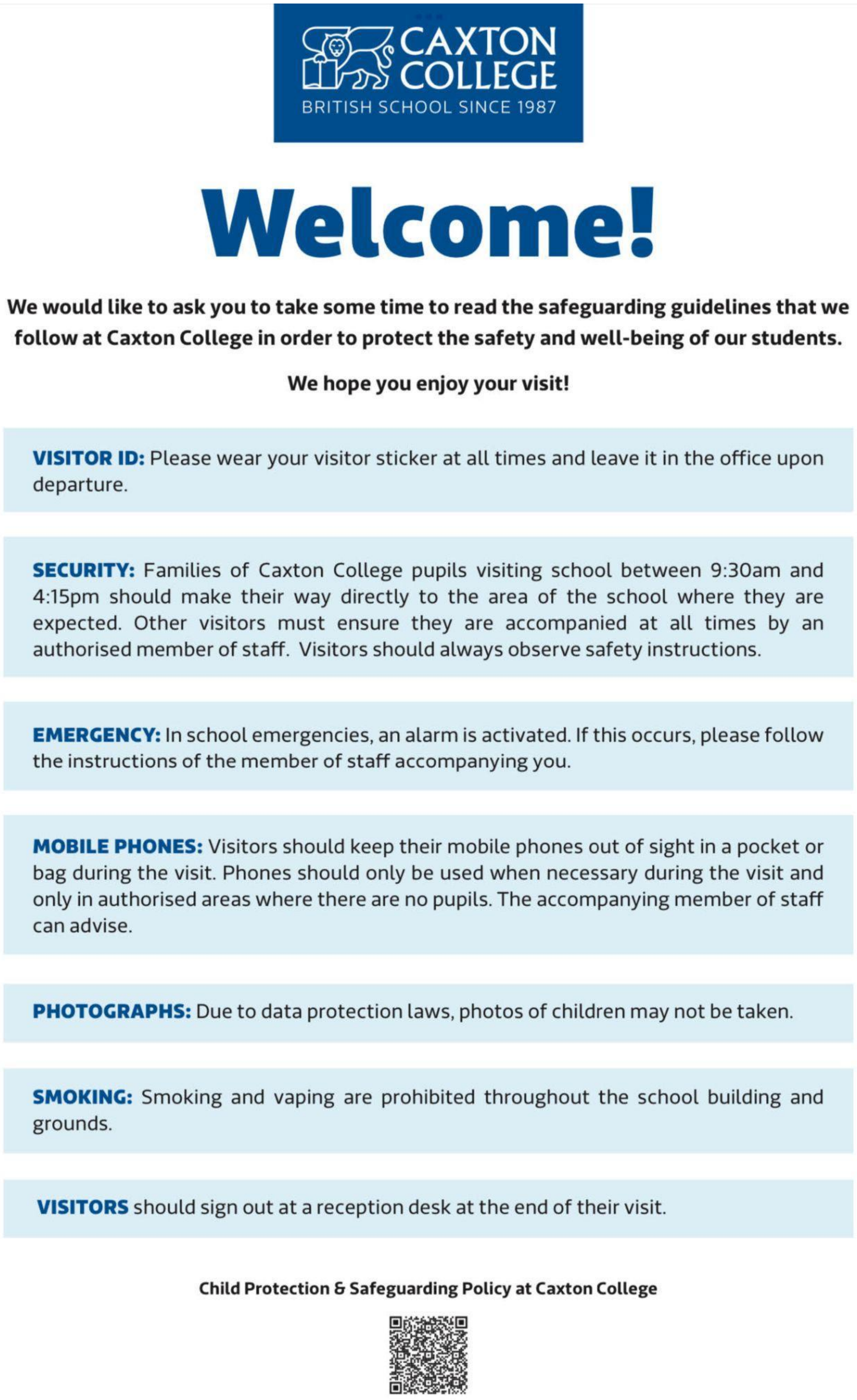
Removal of Remote Access Rights

Access rights for remote access may be changed or removed from any user at any time if there is deemed to be a breach of the conditions of use or the user’s access is compromising the confidentiality, integrity and/or availability of Caxton College´s systems or services.

The remote access rights of all employees and third party users shall be removed upon termination of employment, contract, or agreement.

Appendix F

Safeguarding Guidelines for Visitors



CAXTON COLLEGE
BRITISH SCHOOL SINCE 1987

Welcome!

We would like to ask you to take some time to read the safeguarding guidelines that we follow at Caxton College in order to protect the safety and well-being of our students.

We hope you enjoy your visit!

VISITOR ID: Please wear your visitor sticker at all times and leave it in the office upon departure.

SECURITY: Families of Caxton College pupils visiting school between 9:30am and 4:15pm should make their way directly to the area of the school where they are expected. Other visitors must ensure they are accompanied at all times by an authorised member of staff. Visitors should always observe safety instructions.

EMERGENCY: In school emergencies, an alarm is activated. If this occurs, please follow the instructions of the member of staff accompanying you.

MOBILE PHONES: Visitors should keep their mobile phones out of sight in a pocket or bag during the visit. Phones should only be used when necessary during the visit and only in authorised areas where there are no pupils. The accompanying member of staff can advise.

PHOTOGRAPHS: Due to data protection laws, photos of children may not be taken.

SMOKING: Smoking and vaping are prohibited throughout the school building and grounds.

VISITORS should sign out at a reception desk at the end of their visit.

Child Protection & Safeguarding Policy at Caxton College

CAXTON
COLLEGE