Online Safety Policy
[Paragraphs 7 & 8, Part 3 ISSR]
Bablake and King Henry VIII
Pre-Prep School

Author	Head of Computing and Digital Learning
Version Number	1.1
Approval Date	**March 2023**
Approved By	Full Governing Board
Date of Last Review	March 2024
Review Cycle	Annually
Date of Next Review	**Summer Term 2024**
Date of Next Approval	FGB, Summer Term 2024

Regulatory / Statutory Authority(ies)	▪ The Independent School Standards Regulations (ISSR). ▪ Independent Schools Inspectorate (ISI) - Para 7 & Para 8, Part 3 ISSR – Safeguarding. ▪ Data Protection Act 1998
Related Policies, Procedures, and/or Documentation	▪ Safeguarding and Child Protection Policy ▪ Acceptable Use (of ICT) Policy ▪ Behaviour Policy ▪ Anti-Bullying Policy
Published To	☐ CSF Website ☒ School Website ☒ Shared Staff Area ☒ ISI Portal ☒ Available to Parents

VERSION HISTORY

Version Number	Amendment(s) Or Formal Review	Date [Month/Year]	Summary of change(s)
1.0	Formal Review	March 2023	Formal Review and Approval at Full Governing Board
1.1	Update	March 2024	Updated Role Descriptors / Titles; Converted to new policy template and structure. AUP Appendices added.
2.0	*Formal Review*	*March/April 2024*	*In progress with Head of ICT ahead of FGB, Summer Term*

TABLE OF CONTENTS

This policy applies to Bablake and King Henry VIII Pre-Prep, including Early Years and Bablake Junior School.

1 Statement of General Principles

Bablake and King Henry VIII Pre-Prep and Bablake Junior recognise that Computing and Digital Learning are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using Computing to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and Computing is seen as a responsibility and that pupils, staff and parents use it appropriately and practise good e-safety. 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.

Online safety 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. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography, or face-to-face meetings. There is a 'duty of care' for any persons working with children and educating all members of the school community on the risks and responsibilities of online safety falls under 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 Computing activity in school and provide a good understanding of appropriate Computing 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 applies to all aspects of the schools including those covering Early Years.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures.

2 Roles and Responsibilities

The school online safety is coordinated in collaboration with the Head of Computing and Digital Learning, the Head of Junior School, Head of Pre Prep and the Deputy Head Pastoral (Designated Safeguarding Lead – DSL). The Deputy Head Pastoral will take on the responsibility of Digital Defender Lead. The Digital Defenders are a group of Year 5 and 6 pupils that help to develop pupil awareness of online safety through assemblies and pupil-led lessons.

The designated member of the governing body responsible for online safety is Mr Phil Healy, Governor with responsibility for Child Protection and Safeguarding.

2.1 Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing e-safety incidents and monitoring reports. Online safety falls

within the remit of the governor responsible for Safeguarding. The role of the online safety governor will include to:

- ensure an online safety policy is in place and is available to all stakeholders;
- ensure that there is an online safety coordinator who has been trained to a higher level of knowledge which is relevant to the school, up to date and progressive;
- ensure that procedures for the safe use of Computing and the Internet are in place and adhered to; and to
- hold the Head and staff accountable for online safety.

3 The Heads and Senior Leadership Team (SLT)

The Heads have a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be managed collaboratively by Head of Computing and Digital Learning, the Head of Junior School, Head of Pre Prep and the Deputy Head Pastoral (Designated Safeguarding Lead – DSL). Any complaint about staff misuse must be referred to the Head of Computing and Digital Learning at the school or, in the case of a serious complaint, to the Head. The role of the Heads and SLT will include to:

- ensure access to induction and training in online safety practices for all users;
- ensure appropriate action is taken in all cases of misuse;
- ensure that Internet filtering methods are appropriate, effective, and reasonable;
- ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SLT;
- ensure that pupil or staff personal data as recorded within school management system sent over the Internet is secured; and to
- ensure the school Computing system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

4 Digital Defender Lead:

The role of the Digital Defender Lead is to:

- Lead E-safety meetings.
- Work in partnership with Head of Computing and Digital Learning to ensure systems to protect pupils are reviewed and improved.
- Ensure the school Computing system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.
- Receive reports of e-safety incidents and creates a log of incidents to inform future online safety developments,
- Report to Senior Leadership Team.

5 Head of Computing and Digital Learning:

The role of the Head of Computing and Digital Learning is:

- to work in partnership with the school's IT team to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- to ensure that the school meets required online safety technical requirements and any relevant body online safety policy / guidance that may apply;
- to ensure that users may only access the networks and devices through a properly enforced password protection policy;
- to ensure that the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person;
- to keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant; and
- to ensure that 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 Deputy Head Pastoral / Head; for investigation / action / sanction.

6 Communicating School Policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. Online safety is integrated into the curriculum in any circumstance where the Internet or technology are being used, and during Computing and PSHE lessons where personal safety, responsibility, and/or development are being discussed.

7 Making Use Of Computing and the Internet In School

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary Computing skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

7.1 The Benefits of using Computing and Internet in Schools:

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

7.1.1 For Pupils

- Unlimited access to worldwide educational resources and institutions such as art galleries, museums, and libraries.

- 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.

7.1.2 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 pupils and parents.
- Class management, attendance records, schedule, and assignment tracking.

7.1.3 For parents

- As a source of information to provide educational support at home.
- To enable effective communication between home and school.

8 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. Pupils 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.

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 Head of Computing and Digital Learning. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

9 Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and Internet networks as a whole 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 Bablake School IT Team 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 or taken off site can be encrypted;
- making sure that unapproved software is not downloaded to any school computers. Alerts will be set up to warn users of this;
- 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;
- portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team.

More information on protecting personal data can be found in **section 11** of this policy.

10 Emails

The school uses email internally for staff and pupils, and externally for contacting parents, and it is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally; and
- providing immediate feedback on work, and requests for support where it is needed.

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, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their contents but will only do so if it feels there is reason to.

10.1 School Email Accounts and Appropriate Use

At Bablake Junior we recognise that is it is unwise to assign pupils' school email addresses that state their full name and the school name, as this makes them more vulnerable to being identified by unsuitable people. Key Stage 2 children have an email address which is used to access Microsoft Teams. Restrictions are in place to prevent children from emailing outside of the Bablake system and other people emailing into their accounts.

10.2 Staff Using Email in School:

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 representing the school at all times and should take this into account when entering into any email communications.
- Staff must tell a member of the senior 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.
- The forwarding of chain messages is not permitted in school.

10.3 Pupils Using Email in School:

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the Computing curriculum and in any instance where email is being used within the curriculum or in class:

- 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 either from within the school or from an external account. 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 through the Computing curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

11 Published Content and the School Website

The school website and Facebook page are viewed as useful tools for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, pupils, 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, and details for contacting the school will be for the school office only. **For information on the school policy on children's photographs on the school website please refer to section 11.1 of this policy.**

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

Colour photographs and pupils' work bring our school to life, showcase our pupils' 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 Data Protection Act 1998 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. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to.

11.2 Using Photographs of Individual Children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify pupils or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school's permission. The school follows general rules on the use of photographs of individual children:

- Parental consent must be obtained. Consent will cover the use of images in:
  - all school publications;
  - on the school website;
  - in newspapers as allowed by the school.
- Electronic and paper images will be stored securely.
- Names of stored photographic files will not identify the child.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils (i.e. a pupil in a swimming pool, rather than standing by the side in a swimsuit).
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Events recorded by family members of the pupils such as school plays or sports days must be used for personal use only.
- Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them, or they are being asked to participate in.

- Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils. For more information on safeguarding in school please refer to our school **Child Protection and Safeguarding policy.**

11.3 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 school's **Safeguarding and Child Protection Policy** and **Behaviour Policy.**

Our pupils increasingly use electronic equipment on a daily basis to access the internet and share content and images via social networking sites such as Facebook, Twitter, MSN, Tumblr, Snapchat and Instagram. We recognise that some pupils at Bablake Junior use these sites although they are all younger than 13 and therefore include safety education in our curriculum.

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.

Cyberbullying and sexting by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures (as found in our **Anti-bullying Policy**). Serious incidents may be managed in line with our child protection procedures.

Many pupils own or have access to handheld devices and parents are encouraged to consider measures to keep their children safe when using the internet and social media at home and in the community.

11.4 Social Networking, Social Media and Personal Publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school.

Social media sites have many benefits for both personal use and professional learning; however, both staff and pupils should be aware of how they present themselves online. Pupils are taught through the Computing curriculum and PSHE 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. They are all made fully aware of the Acceptable Use (of ICT) Policy (AUP) regarding the use of Computing and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- 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 representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.

12 Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace in today's society, 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;
- 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. Some of these are outlined below.

- 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. For more information on the school's disciplinary sanctions read the school **Behaviour Policy.**
- 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.
- Mobile phones must be handed in at the school office by any pupil upon arrival at school.
- Any pupil who brings a mobile phone or personal device 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.
- Images or files should not be sent between mobile phones in school.
- If staff wish to use these devices in class as part of a learning project, they must get permission from a member of the senior leadership team.

12.1 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.

Staff

- If staff use their own personal devices to contact pupils or parents either in or out of school time, it must be communicated through school email or Teams. Staff are discouraged from sharing their personal mobile numbers with parents.
- If staff use their personal devices to take photos or videos of pupils for educational purposes, these photos and videos must be immediately deleted from these devices once photos or video has been safely uploaded to the school network.
- The school expects staff to lead by example. Personal mobile phones can be used during school hours. However, these devices should not be used in the presence of pupils.
- No mobile phones are permitted in the Early Years Foundation Stage (EYFS)
- Any breach of school policy may result in disciplinary action against that member of staff. More information on this can be found in the **Child Protection and Safeguarding Policy**, or in the staff contract of employment.

13 Cyberbullying

The school, as with any other form of bullying, takes Cyberbullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the **Behaviour Policy** and **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 follow its **Anti bullying Policy** and:

- 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 in order to identify the bully;
- record and report the incident;
- provide support and reassurance to the victim; and
- 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 whole 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.

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 provide may be contacted to do this if they refuse or are unable to remove it. They may have their Internet access suspended in school.

Repeated bullying may result in fixed-term exclusion.

14 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.

15 Protecting Personal Data

Bablake and King Henry VIII Pre-Prep and Bablake Junior believe 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 in order 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 the data is collected, what is collected, and how it is used. Assessment data, 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 pupils.

In line with the Data Protection Act 1998, 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 longer than is necessary;
- process the data in accordance with the data subject's rights;
- ensure that data is secure; and
- 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 pupils or staff to pass information onto external authorities, for example, our local authority, Ofsted, or the Department of Health. These authorities 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.

16 Review, Approval & Publication

The Head of Computing and Digital Learning has strategic oversight of this policy which is reviewed every year unless otherwise required owing to a change in policy/legislation or guidance; once reviewed, the policy is presented to the Education Oversight Committee for their formal recommendation to present it to the Full Governing Board for final approval.

This Policy will also be made available to parents/carers via the Schools' website; and, published to the ISI Portal.

17 Related Policies and Procedures

This policy may need to be read in conjunction with the following Foundation/School policies:

- Safeguarding and Child Protection Policy
- Acceptable Use (of ICT) Policy
- Behaviour Policy
- Anti-Bullying Policy

And/or with reference to the following legislation or governance provisions:

- The Independent School Standards Regulations (ISSR).
- Independent Schools Inspectorate (ISI) - Para 7 & 8, Part 3 ISSR – Welfare, Health and Safety of Pupils.
- Data Protection Act 1998

18 Appendices

Included in this policy:

- Appendix 1: Acceptable Use of ICT (Remote Learning)
- Appendix 2: Acceptable Use of ICT Policy

END

18.1 Appendix 1: Acceptable Use of ICT (Remote/Online Learning) Policy

ACCEPTABLE USE OF ICT (REMOTE LEARNING) POLICY (AUP)

Core Values:

Safety Responsibility Respect Honesty Integrity

POLICY AGREEMENT

Principles

- We are aiming to continue to provide an excellent education to all of our pupils.
- Interacting with each other on-line is no different than interacting face-to-face: we are required to maintain the principles of respect, dignity, prudence, concern for and protection of others, and safety in all interactions.

General Conduct

- Pupils must conduct themselves in the same way they would in school.
- Language, both spoken and written, should remain appropriate and suitably academic.
- We continue to expect the highest standards of politeness and integrity from our pupils.
- We expect pupils to access their full curriculum as much as they are reasonably able to.
- We expect pupils to meet all deadlines set by staff for the submission of work unless affected by illness or other extenuating factors.
- Pupils must respect the privacy of others and so must 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.

Conduct in 'Live' Lessons (Meetings)

- Meetings will only occur with a minimum of three people present, including at least one teacher.
- Pupils may join any Meeting occurring in their normal class Team.
- Pupils must leave a Meeting when instructed to do so.
- Staff will advise pupils of when Meetings will occur in advance, where possible this will be in a normal lesson slot.
- Pupils should only enable microphones with teacher permission.
- Pupils should be mindful of the appropriateness of possible background sound when using their microphone.
- Meeting text chats should only be used for learning conversations as directed by the teacher; these chats are logged within Teams.
- Pupil cameras will be enabled as a default setting.
- We expect pupils to adhere to the following guidelines for use of their camera:

- choose an appropriate location, not a bedroom;
- choose a location where other people will not appear on camera without realising;
- blur the background or add a false background using the video settings within teams;
- if this is not possible, choose a location with a plain background;
- be appropriately dressed at all times;
- only turn on the camera if the teacher gives permission and only ever after the live lesson has started;
- be prepared to turn the camera off immediately if requested to do so;
- do not use the camera as a way of communicating with others during lessons;
- only use a camera if you are comfortable doing so.

Use of Shared Resources

We expect that all resources shared by members of staff are only used as directed and on the platforms provided by Bablake. In particular, if resources are shared, including audio and video, pupils must not:

- take screenshots;
- share content outside of the Team;
- record any part of a lesson or video;
- post any content on to another site/platform;
- share any of the resources outside of the school.

Sanctions

- Teachers will report unacceptable behaviour to Deputy Head Pastoral or Head of Computing and Digital Learning.
- In the event of unacceptable conduct, we will continue to use the schools behaviour policy to sanctioning behaviour. This may include:
  - removing pupils from live Meetings;
  - limiting pupil contribution rights in Teams;
  - removing pupil access to live Meetings;
  - removing pupil access to any/all shared resources.
- Upon our return to normal school life sanctions may be administered in light of pupil conduct during our period of closure

END

18.2 Appendix 2: Acceptable Use of ICT Policy (Onsite Learning)

ACCEPTABLE USE OF ICT POLICY (AUP)

Core Values:

Safety Responsibility Respect Honesty Integrity

POLICY AGREEMENT

Personal Safety

Please read these statements and confirm your agreement:

- I will keep my username and password safe and secure and not share it with anyone else.
- I will not log on as anyone else; I will not use any other person's username or password.
- I will not share personal information about myself or others when online (this could include my name, address, age, gender, school, my friends' names or information about my family, etc.).
- I will immediately tell any adult if anything online makes me feel sad or uncomfortable.
- I understand that school will monitor my use of school computers and will share with my teacher or parents anything they are worried about.

NB

- **I will not change any device settings.**
- **I will not arrange to meet people offline that I have only met online.**

Responsible Use

Please read these statements and confirm your agreement:

- I will not eat or drink in computer areas as spillage can cause serious damage to hardware.
- I understand that school computers and accounts are just for school work.
- I will not download or upload files without checking with my teacher.
- I will delete files from my area that I no longer require.
- I will not share files that are inappropriate or will cause upset to others.
- I will not use any programmes or software I have not been told to use.
- I will not use school computers or accounts for social networking, online gaming, online gambling, internet shopping, file sharing or video broadcasting (e.g. YouTube).
- I will not bring or use my own personal devices (mobile phones/USB devices, etc.) in school without permission. I understand that, if I am allowed to use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not click on any links or go on any websites without permission from my teacher.
- I will not install or attempt to install or store programmes of any type on any school device.
- I will alter any computer settings.
- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's permission.
- I will immediately report any damage or faults involving equipment or software; however, these may have happened.

Respectful Communication

Please read these statements and confirm by ticking the box below:

- I will be polite and responsible when I communicate with others.
- I will use kind language when communicating online.
- I will not use inappropriate language when naming files or choosing passwords.
- I will not take or distribute images of anyone without their permission.
- I will not share or store personal and private information on school devices.

NB. We expect that you will uphold this standard of behaviour when you communicate with members of our community outside of school and act with respect, courtesy and integrity at all times.

Digital Honesty

Please read these statements and confirm by ticking the box below:

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

- I should ensure that I have permission to use the original work of others in my own work.
- I will not try to download copies of other people's work (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I understand that not everything I read online is true, and that the work of others may not be honest and may be a deliberate attempt to mislead me.

PARENT AND STUDENT CONFIRMATION

Sanctions

I understand that if I fail to comply with this Acceptable Use Policy Agreement (AUP) I will be subject to disciplinary action in accordance with the schools 'stepped approach to discipline' as set out in the School Code of Conduct and Behaviour Policy. This may include detentions, suspensions, fixed term or permanent exclusion, contact with parents and, in the event of illegal activities, involvement of the police and/or the Local Safeguarding Children's Board.

Signed by:	**Endorsed by:**
_____	_____
Pupil name:	**Parent name:**
_____	_____
Date:	**Date:**
_____	_____

END