BROCKHURST & MARLSTON HOUSE SCHOOLS

Including all of the Pre-Prep Department and Early Years Foundation Stage

ICT & ESAFETY POLICY

Brockhurst & Marlston House Schools (the School) is committed to providing the best possible care and education to its pupils, and to safeguarding and promoting the welfare of children and young people. This policy is written with that commitment in mind, and in accordance with KCSIE September 2025.

Reviewed: September 2025
Next Review: September 2026

Brockhurst & Marlston House Schools ICT and eSafety Policy was developed and agreed by the whole staff and has the full agreement of the SLT.

Purpose

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's database. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature attitude.

Benefits

- access to world-wide educational resources including museums and art galleries.
- educational and cultural exchanges between pupils world-wide.
- access to professional bodies and experts in many fields for pupils and staff;.

Internet Use and External Agencies

The school Internet access will be designed expressly for pupil use and will include filtering provided by the Exa-Education (Surf Protect) and be appropriate to the age of pupils. The school will work in partnership with parents, the Local Authority or third party provider, DfE and the Internet Service Provider (GigaClear) to ensure systems to protect pupils are reviewed and improved. Pupils will be taught what is acceptable and what is not acceptable and given clear objectives regarding internet use. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

The school, where possible, will ensure that the use of internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Guest Wi-Fi Provision

The School provides a guest Wi-Fi service for visitors. This network is technically separate from the staff and pupil networks and does not include the School's filtering or monitoring systems. For safeguarding reasons, pupils are not permitted to access the guest Wi-Fi under any circumstances.

All guest Wi-Fi access is subject to the School's ICT and eSafety Policy and is provided for reasonable use by visitors only. Access is not to be used for illegal, inappropriate, or excessive activity. Guest Wi-Fi passwords are changed regularly and provided at the School's discretion.

The School reserves the right to restrict or withdraw access to the guest Wi-Fi at any time.

Safeguarding

All staff receive appropriate online training with updates sent out by the Head of ICT at least annually. All staff should be aware of indicators of abuse and neglect online. Children can abuse other children online and this can take the form of abusive and harassing messages. Sexual abuse can take place online and technology can be used to facilitate offline abuse.

The school uses Surf-Protect by Exa-Education which provides proxy cloud based filtering. If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the Head of ICT.

The DSL and Head of ICT will check the monitoring software daily (AB Tutor Cloud), which provides cloud-based monitoring of all pupils' school Google accounts, Chromebooks, and IT room PCs. Alerts and logs are accessible remotely, allowing proactive safeguarding oversight. All pupil devices and accounts are linked to the monitoring platform and can be reviewed securely by the Head of ICT. Termly reviews of filtering and monitoring logs are documented and retained by the DSL and Head of ICT as part of safeguarding evidence for inspection purposes.

e-mail

Pupils may only use the approved Brockhurst & Marlston House School e-mail accounts on the school system. Pupils must immediately tell a teacher if they receive offensive e-mails. Pupils must not reveal personal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication. Pupils' email addresses only allow @brockmarl.org addresses to send emails to them. Specific email addresses are able to be added to this whitelist – for example: TeenTips or parents' email addresses.

Chatrooms

Pupils will not be allowed access to public or unregulated chat rooms.

Emerging Internet Uses

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils will not be allowed mobile phones or any other device that has cellular capabilities during school time. Any mobile phones brought inadvertently into school should be kept in the school office during the school day. The sending of abusive or inappropriate text messages is forbidden. Full boarders may have a mobile phone. Please refer to the boarding polices.

Internet access authorisation

The school allows Internet access to all staff and pupils. All pupils will be asked to sign a consent form. In the Foundation Phase, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Inappropriate Material

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. Surf Protect by Exa Education provides a cloud based proxy filtering system that filters content considered unsuitable for an educational setting and this is reviewed regularly.

Filtering and Monitoring

At Brockhurst School, safeguarding the online environment for our pupils and staff is paramount. The proprietor plays a crucial role in implementing robust filtering and monitoring measures that align with the stringent safety and security standards we uphold. With support from the senior leadership team and the DSL, we ensure meticulous adherence to these standards, fostering a safe and nurturing online atmosphere. Every member of our team, including staff and third-party entities, is well-versed in their roles and responsibilities, guaranteeing swift and effective responses to any online security challenges. These roles are clearly defined, adaptable, and inclusive, ensuring comprehensive oversight even when specialised personnel is not available.

Collaboration is at the heart of our approach to online safety. Senior leaders and the proprietor join forces with the Designated Safeguarding Lead (DSL), Head of ICT and IT service providers to cultivate a secure and supportive online learning environment. The DSL is specifically tasked with online safety, working in tandem with the Head of ICT and IT professionals to ensure the integrity and reliability of our filtering and monitoring systems. Whether managed in-house or outsourced, our IT service providers play a pivotal role in maintaining system integrity, generating insightful reports, and addressing system checks and concerns swiftly. This harmonious collaboration ensures Brockhurst School meets and exceeds compliance standards, nurturing a safe, secure, and conducive learning atmosphere.

Furthermore, the commitment to a termly review of our filtering and monitoring systems underscores our pledge to the dynamic and evolving needs of our learning environment. The proprietor ensures that these reviews are exhaustive and insightful, informing necessary adaptations and improvements. By incorporating these reviews into a broader online safety analysis, we harness insights from the senior leadership, the DSL, and IT service providers, ensuring that every perspective is considered and every challenge addressed. These meetings are documented, offering a transparent and accessible overview of our online safety landscape to all. Every aspect, from the specific technological needs of our pupils and staff to the diverse risk profiles and digital resilience of our students, is carefully assessed and addressed.

Brockhurst School is unwavering in its commitment to the highest standards of online safety and security. Our review process is comprehensive, integrating insights on the filtering system's specifications, outside safeguarding influences, and relevant safeguarding reports. Adjustments to the filtering and monitoring protocols are informed, adaptive, and responsive, ensuring the school's readiness for emerging technological and security trends. Every staff member is equipped with the knowledge and tools to uphold the system's integrity, with new devices and services rigorously vetted for compliance before integration. Each step, from the logs to the adaptive review of policies, underscores Brockhurst School's unyielding commitment to a safe, secure, and enriching learning environment for every pupil.

Current Monitoring software: AB Tutor Cloud (monitoring all pupil Google accounts, Chromebooks and PCs)

Current Filtering: Google SafeSearch, Google SchoolApps and SurfProtect

Roles for Filtering & Monitoring

The Head of ICT is responsible for managing, reviewing, updating and overseeing filtering and monitoring systems.

Prevent Duty

Up to date filtering has been put in place to safeguard the pupils from accessing terrorist and extremist material while online. In the same way that teachers are vigilant about signs of possible physical or emotional abuse in any of their pupils, if teachers have a concern for the safety of a specific pupil at risk of radicalisation, they should follow the school's safeguarding procedures which includes discussing it with the school's Designated Safeguarding Lead or in their absence the deputy.

The pupil's internet use is supervised and monitored by a member of staff and inappropriate known website including Virtual Private Network (VPN) sites are blocked. Every staff member at Brockhurst & Marlston House has completed the Channel General Awareness module.

Pupils are taught about the safe use of social media in ICT lessons was well as PSHEE lessons and where to go to for help and support if there is a concern.

Introduction of the policy to pupils

From Year 2 at least one lesson each term will be taught responsible Internet use and eSafety will be taught for both school and home use. This will introduce and/or re-emphasise the school internet access agreement and internet access rules. Rules for internet access will be posted in the ICT Room. Pupils will be informed that internet use will be monitored. Instruction in responsible and safe use should precede any internet access.

Staff

All staff must accept the terms of the 'Electronic Device Acceptable Use Agreement' policy before using any internet resource in school. All staff including teachers, supply staff, teaching assistants, support staff and administrative staff will have access to the School ICT and eSafety Policy, and its importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Professional conduct is expected.

ICT system security

The school ICT systems will be reviewed regularly with regard to security and any DfE guidance will be adopted. Unapproved system utilities and executable files will be blocked in pupils' work areas by the Active Directory environment. Only ICT technicians will be able to introduce and install new programs onto the network.

Complaints

Responsibility for handling incidents will be delegated to a senior member of staff. Any complaint about staff misuse must be referred to the Headmaster. Parents will be informed should a pupil misuse the Internet.

Parents

Parents' attention will be drawn to the School ICT and eSafety Policy in emails and on the school Web site. Internet issues will be handled sensitively to inform parents without undue alarm. Further information and support for parents can be found on the school website in the Helpful Advice for Parents at http://www.brockmarl.org.uk/keeping-children-safe-helpful-advice-for-parents/107.html

Teaching and Learning Purpose

This policy reflects the school values and philosophy in relation to the teaching and learning of ICT. It sets out a framework within which teaching and non-teaching staff can operate and gives guidance on planning, teaching and assessment.

The policy should be read in conjunction with the scheme of work for ICT, which sets out in detail what pupils in different classes and year groups will be taught and how ICT can facilitate or enhance work in other curriculum areas.

Introduction

Information and Communications Technology prepares pupils to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology.

We recognise that Information and Communications Technology is an important tool in both the society we live in and in the process of teaching and learning. Pupils use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discrimination. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of sources.

Our vision is for all teachers and learners in our school to become confident users of ICT so that they can develop the skills, knowledge and understanding which enables them to use appropriate ICT resources effectively as powerful tools for teaching & learning.

Aims

- To enable children to become autonomous, independent users of ICT, gaining confidence and enjoyment from their ICT activities
- To develop a whole school approach to ICT ensuring continuity and progression in all strands of the ICT National Curriculum
- To use ICT as a tool to support teaching, learning and management across the curriculum

- To ensure ICT is used, when appropriate, to improve access to learning for pupils with a diverse range of individual needs, including those with SEN and disabilities
- To maximise the use of ICT in developing and maintaining links between other schools, the local community including parents and other agencies

Objectives

In order to fulfil the above aims it is necessary for us to ensure:

- a continuity of experience throughout the school both within and among year groups
- the systematic progression through the school
- that all children have access to a range of ICT resources
- that ICT experiences are focussed to enhance learning
- that cross curricular links are exploited where appropriate
- that children's experiences are monitored and evaluated
- that resources are used to their full extent
- that resources and equipment are kept up to date as much as possible
- that staff skills and knowledge are kept up to date

Curriculum Development & Organisation

Each class is allocated a time in the ICT suite to accomplish their ICT work. Each class can be allocated additional time in the computer suite to apply the use of ICT to other subject areas. A weekly timetable is displayed within the Staff room for staff to sign up for additional time where appropriate.

Individual machines in classrooms support the development of ICT capability by enabling further development of tasks from the ICT room; encourage research, and allow for the creative use of ICT in subjects. This is highlighted in the ICT plan and in subject plans.

Digital projectors and Interactive White Boards (IWBs) are located in some of the classrooms as well as the ICT suite. These are used as a teaching resource across the curriculum.

Teaching & Learning

Teachers' planning is differentiated to meet the range of needs in any class including those children who may need extra support, those who are in line with average expectations and those working above average expectations for children of their age.

A wide range of styles are employed to ensure all children are sufficiently challenged:

- Termly eSafety lessons are taught in groups and individually.
- Children may be required to work individually, in pairs or in small groups according to the nature or activity of the task.
- Different pace of working.
- Different groupings of children - groupings may be based on ability either same ability or mixed ability.
- Different levels of input and support.
- Different outcomes expected.

The Head of ICT will review teachers' ICT plans to ensure a range of teaching styles are employed to cater for all needs and promote the development of ICT capability.

Equal Opportunities

All pupils, regardless of race, class, gender or transgender, should have the opportunity to develop ICT capability.

It is our policy to ensure this by:

- ensuring all children follow the scheme of work for ICT
- keeping a record of children's ICT use to ensure equal access and fairness of distribution of ICT resources
- providing curriculum materials and software which are in no way class, gender or racially prejudice or biased
- monitoring the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged

The school actively encourages parents in developing their knowledge of curriculum requirements for ICT and how they can support their children.

Internet Safety (eSafety)

Internet access is planned to enrich and extend learning activities.

The school has acknowledged the need to ensure that all pupils are responsible and safe users of the Internet and other communication technologies. An Acceptable Internet Code of Conduct has thus been drawn up to protect all parties and rules for responsible internet use, which will be displayed in the ICT room.

The school will do all that we reasonably can to limit children's exposure to harmful and inappropriate online material, with appropriate filters and monitoring systems in place; we are also cautious against 'overblocking' and imposing unreasonable restrictions.

Although the school offers a safe online environment through filtered internet access we recognise the importance of teaching our children about online teaching and safeguarding and their responsibilities when using communication technology.

We have developed this as part of our ICT lessons and PSHEE provision in the whole school.

Incidents of online bullying or abuse are addressed in line with the school's Anti-Bullying Policy, which outlines procedures for reporting, investigation and support.

Use of Artificial Intelligence (AI)

The School recognises that Artificial Intelligence (AI) technologies are increasingly accessible to pupils and staff, and that they can provide opportunities to enhance teaching and learning. However, the School is also aware of the potential risks that AI tools present in terms of safeguarding, misinformation, data protection and academic integrity.

- **Educational Use**: AI may be used to support learning, creativity and problem-solving under staff supervision. Pupils will be encouraged to use AI critically, understanding both its potential and its limitations.

- **Safeguarding and Online Safety**: AI-generated content can be inaccurate, biased or harmful. Pupils will be taught to evaluate AI outputs carefully and will be made aware of risks such as

deepfakes, misinformation, genAI (generative AI in the form of text or image) and inappropriate content. The School's filtering and monitoring systems apply to AI platforms in the same way as to other online services.

- **Data Protection**: Pupils and staff must not enter personal data, images or confidential school information into AI systems. The School will ensure that any use of AI is consistent with data protection legislation, including GDPR.

- **Academic Integrity**: Work produced with the assistance of AI must not be presented as a pupil's own independent work. The School will educate pupils about responsible use and will address any misuse in line with the behaviour policies.

- **Staff Responsibilities**: Staff are expected to model safe and appropriate AI use, ensuring that AI is introduced in the classroom in a way that supports learning and does not replace independent thought or effort.

- **Curriculum Integration**: AI is included within e-safety and digital literacy teaching. Pupils are encouraged to develop critical thinking skills to question the accuracy, bias and purpose of AI-generated information.

- **Prevent Duty**: The School recognises that AI can be exploited to generate harmful or extremist material. The School's safeguarding approach ensures that any such risks are managed in line with Prevent and child protection policies.

Cybersecurity

The School recognises that cybersecurity is a safeguarding priority. A cyber incident could compromise pupil safety, disrupt learning, or expose personal data.

- **Responsibilities**
  The Proprietor and Senior Leadership Team ensure effective cybersecurity arrangements. The Head of ICT manages the systems. All staff must follow school protocols, use secure passwords, report concerns, and avoid installing unauthorised software.
- **Risk Management**
  The School conducts regular cybersecurity risk assessments and maintains safeguards against threats such as phishing, malware, and unauthorised access. We use F-Secure to protect devices and networks, and our arrangements are audited using 360safe. The Proprietor reviews these measures as part of safeguarding oversight.
- **Incident Response**
  Any suspected cyber incident must be reported immediately to the Head of ICT and the Designated Safeguarding Lead (DSL). All incidents are investigated, and escalated in line with safeguarding and data protection procedures, with statutory reporting where required.
- **Training and Awareness**
  Staff receive training at induction and through regular updates, covering secure data use, recognising threats, and reporting concerns. Pupils are taught digital resilience through the curriculum, including online safety, password security, and recognising scams.

Assessment

Formative assessment occurs on a lesson by lesson basis based on the lesson objectives and outcomes in the scheme of work. These are conducted informally by the class teacher and are used to inform future planning.

Inclusion

We recognise ICT offers particular opportunities for pupils with special educational needs and gifted and/or talented children and /or children with English as an additional language for example.

ICT can cater for the variety of learning styles which a class of children may possess.

Using ICT can:

- increase access to the curriculum
- raise levels of motivation and self esteem
- improve the accuracy and presentation of work
- address individual needs

We aim to maximise the use and benefits of ICT as one of many resources to enable all pupils to achieve their full potential. If the situation arises, the school will endeavour to provide appropriate resources to suit the specific needs of individual or groups of children.

Roles & responsibilities

Senior Leadership Team

The overall responsibility for the use of ICT rests with the Senior Leadership Team of a school. The Head, in consultation with staff:

- determines the ways ICT should support, enrich and extend the curriculum.

- decides the provision and allocation of resources .
- decides ways in which developments can be assessed, and records maintained .
- ensures that ICT is used in a way to achieve the aims and objectives of the school.
- ensures that there is an ICT policy, and identifies a Head of ICT.

Head of ICT

There is a designated Head of ICT to oversee the planning and delivery of ICT within the school.

The Head of ICT will be responsible for

- raising standards in ICT as a subject.
- facilitating the use of ICT across the curriculum in collaboration with all Head of Department.
- providing or organising training to keep staff skills and knowledge up to date.
- advising colleagues about effective teaching strategies, managing equipment and purchasing resources.
- ensuring the school filtering system is functioning.
- monitors all pupil computer use on a daily basis.

Heads of Department

There is a clear distinction between teaching and learning in ICT and teaching and learning with ICT. Subject coordinators should identify where ICT should be used in their subject schemes of work. This might involve the use of short dedicated programs that support specific learning objectives or involve children using a specific application which they have been taught how to use as part of their ICT study and are applying those skills within the context of another curriculum subject.

The Classroom Teacher

Even though whole school co-ordination and support is essential to the development of ICT capability, it remains the responsibility of each teacher to plan and teach appropriate ICT activities and assist the Head of ICT in the monitoring and recording of pupil progress in ICT.

Health & Safety

We will operate all ICT equipment in compliance with Health & Safety requirements. Pupils will also be made aware of the correct way to sit when using the computer and the need to take regular breaks if they are to spend any length of time on computers.

Appropriate legislation, including copyright and data protection

All software loaded on school computer systems must have been agreed with the Head of ICT.

All our software is used in strict accordance with the licence agreement.

We don't allow personal software to be loaded onto school computers.

Please refer to the school's Data protection policy**.**

Effective and efficient deployment of ICT resources

ICT resources are deployed throughout the school to maximise access, to enhance teaching & learning and to raise attainment.

To enable regular and whole class teaching of ICT the school has an ICT suite, which all classes in key stages 1 & 2 use for one lesson per week to develop their ICT skills.

Social Media Policy

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, Tumblr, Last.fm, Whatsapp, SnapChat, Instagram, PS4 and comment streams on public websites such as newspaper site.

Within this policy there is a distinction between use of school-sanctioned social media for professional educational purposes, and personal use of social media in practice.

1. Personal use of social media

- School staff will not invite, accept or engage in communications with parents or children from the school community in any personal social media whilst in employment at Brockhurst and Marlston House Schools.
- Any communication received from children on any personal social media sites must be reported to the DSL.
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these must immediately be reported as above.
- Members of the school staff are strongly advised to set all privacy settings to the highest possible levels on all personal social media accounts.
- All email communication between staff and members of the school community on school business must be made from an official school Gmail account (@brockmarl.org).
- Staff should not use personal email accounts or mobile phones to make contact with members of the school community on school business, nor should any such contact be accepted, except in circumstances given prior approval by the Headmaster.
- Staff should consider the reputation of the school in any posts or comments related to the school on any social media accounts.
- Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account. The school is aware that there are parents of pupils who are also staff members. In this case they are encouraged to consider their reputation.

2. School-sanctioned use of social media.

- There are many legitimate uses of social media within the curriculum and to support student learning. For example, the school has an official Facebook account. When using social media for educational purposes, the following practices must be observed:
- Staff should set up a distinct and dedicated social media site or account for educational purposes.
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school.
- Care must be taken that any links to external sites from the account are appropriate and safe.
- Any inappropriate comments on or abuse of school-sanctioned social media should immediately be removed and reported to the Headmaster.
- Staff should not engage with any direct messaging of students through social media where the message is not public.

Pupil Acceptable Use Agreement at Brockhurst and Marlston House

This agreement helps keep everyone safe when using technology in school and at home. It applies to all devices, networks, online platforms, and digital resources provided or accessed through the school. By following it, you are helping to protect yourself and others.

Safe and Responsible Use

- I will only use school devices, networks and accounts for schoolwork and learning.
- I will keep my usernames and passwords private and never share them.
- I will always use kind and respectful language online.
- I will not look for, share, or use anything harmful, illegal, or inappropriate.
- I will never share personal information (such as my full name, address, phone number, school details, or photos) without permission from a trusted adult.
- I will only take or share photos, videos, or recordings if I have permission.
- I understand that my school Google account and any device I use it on are monitored for my safety.

Staying Safe

- If something worries me, upsets me, or doesn't seem right online, I will stop and tell a teacher or trusted adult straight away.
- I know that my online activity on school systems is monitored to help keep everyone safe.
- I understand that security systems are there for my safety, and I will not try to change them.

Respecting Others

- I will treat others kindly both online and offline.
- I understand that bullying, cyberbullying, or misuse of technology will not be tolerated and may lead to serious consequences.

If you have any questions about this agreement, please speak to Mr Whitton-Hughes (MiC of ICT, Online Safety Officer) or Mr Raeburn-Ward (DSL).

Agreement

I have read and understood this Acceptable Use Agreement. I agree to follow these rules to help keep myself and others safe.

Pupil Name: _____ **Class:** _____

Signature: _____ **Date:** _____

Pupil AUA updated 09/2025