Jordans School

E-safety Policy

Reviewed: March 2026
Update required: March 2027

Statement of Intent

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, both in and out of the school.

This Policy should be read in conjunction with the following policies: Child Protection, Behaviour, Safeguarding, Remote learning, Anti-Bullying and Data Protection and Keeping Children Safe in Education.

Computing Vision

- Jordans is a forward thinking school that integrates technology throughout lessons, as appropriate, in addition to running discrete Computing lessons. Our aim is that all pupils leave the school confident and proficient in using age appropriate technology while also understanding how to keep safe.
- Children will experience a diverse range of software and hardware and have many opportunities to design and create their own content.
- Children will receive discrete Computing lessons in word processing, graphics and publishing, and coding.
- Opportunities will be sought to use computing to enrich the learning experience of children within the school. Cross-curricular links allow children to apply their digital skills to many other subjects and to learn how to use technology and online tools safely and for suitable timeframes.
- Appropriate software and web based learning sites will be vetted first, and then used if they enhance learning.
- E-Safety will be a continuous area of learning throughout every Computing lesson for every child in the school. All children will be taught to independently question content they experience on the internet and think before they share content digitally.

Computing as it relates to learning and life skills.

- Children will be taught logical thinking skills and to try to predict outcomes based on the knowledge they already have.
- Through the use of planning and algorithms, children will be taught to think sequentially, working through challenges step by step.
- Children will be encouraged to have courage in their learning, whilst keeping internet safe.
- Children will learn to become problem solvers through the regular opportunities given to create their own content and debug their own programs.
- Children will become resilient learners, who see setbacks as opportunities to learn and improve.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Headteacher:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, the Headteacher's role will also be *E-Safety Co-ordinator* as they are the nominated Designated Safeguarding Lead Person.
- The Headteacher and all staff should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles.
- The Headteacher takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Liaises with the Local Authority / relevant body.
- Liaises with technical support company.
- Meets with Safeguarding Governor.

Network Manager:
Jordans School has a managed IT service provided by an outside contractor (Buckinghamshire Council – IT Schools) and it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures. It is also important that the managed service provider is fully aware of the school's e-safety policy and procedures.

The Network Manager and Headteacher are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are changed periodically.
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- attempted misuse to be reported to the Headteacher for investigation / action / sanction.

Teaching and Support Staff:
are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They read weekly Staff Meeting Minutes and weekly information.
- Attend relevant training as directed by Headteacher.
- They have read, understood and signed the Code of Conduct.
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- All digital communications with students / parents / carers are professional and only carried out using official school systems.

- E-safety is embedded in all aspects of the curriculum.
- Pupils understand and follow the e-safety rules.
- They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
- All sites used in lessons are vetted ahead of time by the teacher and only used with pupils if the educational merit is beneficial to their learning and enhances the curriculum.
- In lessons children are not allowed to freely search the internet, rather they are given an appropriate website to navigate and are supervised.
- Appropriate video clips, including movement breaks/yoga/mindfulness guides must be downloaded or saved before showing the children, to avoid pop-up adverts or inappropriate content being shown.
- Safe educational sites – BBC bitesize, CBeebies, National Geographic, Espresso Education and Phonics Play, may be accessed directly.
- A review of class procedures, screen time, educational videos and media will be carried out annually in the Computing staff meeting. E-Safety CPD, training and stakeholder feedback will inform any changes to be made.

Designated Safeguarding Lead Person:
should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults / strangers

  Potential or actual incidents of grooming
- Cyber-bullying
- Anti-terrorism and radicalisation

This policy reflects KCSIE updates, including strengthened filtering and monitoring expectations and explicit recognition of online risks such as misinformation, disinformation and conspiracy theories. The DSL oversees digital safeguarding and ensures staff remain alert to emerging online harms.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupils Code of Conduct.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They should understand the guidance on the taking / use of images and on cyber-bullying.
- Should understand the importance of adopting good e-safety practice when using digital technologies in and out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:
Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' workshops, newsletters and website information about e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events are for private use only and must not be posted on to social media.
- Sign an E-Safety Code of Practice when joining the school (in the Parent Pack).

Training – Governors
Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of teaching and learning -e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Access to training sessions for staff/parents.

Technical – infrastructure / equipment, filtering and monitoring
Jordans School has a managed IT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school, as suggested below. It is also important that the managed service provider is fully aware of the school E-Safety Policy and Acceptable Use Agreements.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restrITed.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Headteacher who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every term.
- The IT service provider is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users by the school's IT service. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The school has provided differentiated user-level filtering (staff / pupils).
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person (service provider portal).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed Acceptable Use Policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- The school network is used to store lesson plans and resources. Memory sticks are not to be used. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- A secure VPN is used for off-site PPA.

Use of digital and video images
Staff, parents / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should also recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made

publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully on the use of such images.
- Pupils' names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school website, newsletter or any online platform or advertisement.

Data Protection
The GDPR Policy will be followed.

Social Media - Protecting Professional Identity
All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who radicalise, harass, cyberbully, discriminate on the grounds of belief, sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school or local authority.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Illegal Incidents
Any suspicion of illegal activity should be reported to the Headteacher immediately. The Headteacher will then report the matter to the Data Protection Officer, Governors, or First Response, where required. Policies will be reviewed in light of any incidents.

Review

This policy and procedures will be reviewed every year. The governing body may, however, review the policy earlier than this if the government introduces new regulations or if the governing body receives recommendations on how the policy might be improved.

Appendix

Jordans School

IT -Acceptable Use

Technologies provide powerful tools, which open up new opportunities for everyone. They can prompt discussion, promote creativity and stimulate awareness of context to enhancing effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible supervised users.

Parents are requested to sign the permission form below with their child to show their support of the school in this important aspect of the school's work.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Parents, carers and adults in schools should be aware of the potential dangers and be taking measures to ensure safe usage by all. Children at Jordans use the Internet on a regular basis as part of their learning. In school, we have regular e-safety activities to remind children of the importance of keeping themselves safe online.

At home, many children are often given unsupervised access to the Internet. This potentially, allows them to access a range of content (both good and bad) and bring it into their homes.

Here are a few tips:
Keep your device in a shared area and take an active part in what your child is looking at and watching - Talk to your child about what they are doing online and remind them not to interact with strangers, to tell you if they see something that upsets them.

Turn off the function that allows videos to roll on to the next one – this reduces the risk of your child seeing something harmful.

Supervise your child during Remote Learning activities.

TikTok and all other Social Media Sites - Are you aware that many of these sites have a minimum age limit of 13, so our pupils should NOT be using them?

Google Safe Search Kids - This is designed to screen sites that contain sexually explicit content and remove them from your search results. While no filter is 100% accurate, SafeSearch helps you avoid content you may prefer not to see or would rather your children did not stumble across.

The internet is a wonderful place, it can help us to keep in touch with friends and help our learning – but it can also cause harm – to us and to others. It is useful to think of it as a day out at a library, theme park or museum. There will be lots to see, do and learn but to keep safe we must stay with our adults and we do not talk to strangers. We also know that anyone can put information up on the internet so we must check information with our adults to see if it is true. Information we put up on the internet cannot be rubbed out, it stays there forever, so we must think carefully about whether what we type is appropriate and whether it is kind.

Remember help is always available at school if you are having any problems online.
You can always talk to your teacher or another adult at school. We are always here to help you and to keep you safe.

At school we use safesearchkids as a safe, child friendly search engine developed by online safety experts.

PUPILS CODE OF PRACTICE FOR THE USE OF THE INTERNET

- I only use the internet when I am with a teacher or adult.
- I never tell anyone my name, address, telephone number when I am on any website or using an e-mail.
- I do not use the internet to upset people, for example by using bad language, or unkind words.
- I always tell my teacher if I see bad language or unpleasant things while I am online.
- I am always myself and do not pretend to be anyone or anything I am not when I am online.
- I know that my teacher will be looking at the sites I use.
- I understand that I will not be able to use the internet if I do not follow these rules.

E-safety Code of Practice

Parents are requested to sign the permission form below with their child to show their support of the school in this important aspect of the school's work.

We agree to support the school's policy on the use of the Internet.

The school will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

Parents, carers and adults in schools should be aware of the potential dangers and be taking measures to ensure safe usage by all. Children at Jordans use the Internet on a regular basis as part of their learning. In school, we have regular e-safety activities to remind children of the importance of keeping themselves safe online.

Child's Name: _____

Signed (parent/guardian): _____ Date: _____

This form will be held on record for the duration of the child's placement at our school.

Jordans School

Photograph Consent

At Jordans School we sometimes take photographs of pupils in order to demonstrate your child's achievements and celebrate the life of the school, we take photographs as they work and play. Under the 'General Data Protection Regulation' (GDPR) we must ask for you to consent and offer you an easy means to withdraw/amend your consent on behalf of your child at any time. We use these photos in the school's prospectus, on the school's website, school newsletters and on display boards around school.

If we use photographs/videos of individual pupils, we will not use the full name of that child in the accompanying text or photo caption.

We would ask you as a parent to consent on behalf of your child what can be done with their images. If you're not happy to do this, that's no problem – we will accommodate your preferences.

Please tick the relevant boxes below and return this form to the school office via your child's book bag.

I give permission for my child's photograph to be used within school for display purposes, learning journeys, achievement records ☐

I give permission for my child's photograph to be used on the prospectus and newsletter ☐

I give permission for my child to appear in local newspapers and the Jordans Village Newsletter from time to time ☐

I give permission for my child's photograph to be used on the school website ☐

I give permission for my child to have a formal school individual photograph and class photograph. I understand this printed/digital version can be purchased by parents ☐

I give permission for my child to be included in production videos. These may be uploaded to an unlisted and unnamed YouTube account with the link circulated to parents. ☐

I give permission for my child's photo to be used in the Year 2 Yearbook produced when they leave Jordans to move to Junior School ☐

I **DO NOT** give permission for the school to take or use photographs of my child ☐

I understand that I am prohibited of uploading images taken during school events to any social media platforms that contain other people's children.

If you change your mind at any time, you can let us know by emailing office@jordans.bucks.sch.uk

Parent's Name…… Date……

Child's Name ……

Conditions of use

- This form is valid indefinitely from the date you sign it.

- We will not re-use any photographs or recordings a year after your child leaves this school. Historic photographs may remain on our school website.

- We will not use the personal details or names of any child or adult in a photographic image or video, on our website, platforms in our school prospectus or in any of our other printed publications.

- We may include pictures of pupils and teachers that have been drawn by the pupils.

- We may use group or class photographs or footage with very general labels, such as ‘a science lesson’ or ‘making Christmas decorations’.

- We will only use images of pupils who are suitably dressed.

- Websites and social media platforms can be viewed throughout the world and not just in the United Kingdom where UK law applies.

Staff (and Volunteer) Acceptable Use Policy

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of IT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of IT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of IT. I will, where possible, educate the young people in my care in the safe use of IT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the IT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school IT systems (eg laptops, email etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the set break times in an appropriate way.
- I will not reference Jordans School on social media.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images. Where these images are published (eg on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that school items are only stored on the school network and not a memory stick or USB device.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- I will only use AI with the permission of the headteacher, after a discussion in which the benefits are deemed to outweigh the risks.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

All expectations are outlined in Staff Induction, Guidance for Visitors and the Staff Code of Conduct.

Legislation

Jordans school recognises that online safety operates within a clear legal and statutory framework. In general, behaviour that is illegal offline is also illegal online. The following legislation and guidance informs this policy.

Data Protection and Privacy

- **Data Protection Act 2018 & UK GDPR** – governs the collection, storage and use of personal data, including pupil images, digital records and online platforms.
- **Age-Appropriate Design Code (Children's Code)** – requires online services used by children to provide high privacy settings and protect children's data by default.

Online Safety and Harm

- **Online Safety Act 2023** – places duties on online platforms to reduce illegal and harmful content and strengthens protections for children.
- **Communications Act 2003** & **Malicious Communications Act 1988** – offences relating to threatening, offensive or harmful online messages.
- **Computer Misuse Act 1990** – offences relating to unauthorised access, hacking or misuse of computer systems.

Safeguarding and Child Protection

- **Keeping Children Safe in Education (KCSIE)** – statutory guidance outlining schools' responsibilities for online safety, filtering, monitoring and staff training.
- **DfE Filtering and Monitoring Standards (2023)** – sets expectations for safe and effective filtering and monitoring systems in schools.
- **Sexual Offences Act 2003** & **Serious Crime Act 2015** – offences including grooming, sexual communication with a child, and sharing indecent images.
- **Protection of Children Act 1978** – offences relating to creating, possessing or distributing indecent images of children.
- **Voyeurism (Offences) Act 2019** – criminalises upskirting and related image-based abuse.

Behaviour, Conduct and School Powers

- **Education and Inspections Acts 2006 & 2011** – powers to regulate pupil behaviour off-site, including online behaviour, and to search and delete data on electronic devices.
- **Searching, Screening and Confiscation Guidance (DfE 2022)** – sets out lawful powers to search pupils and examine digital content.

Harassment, Abuse and Hate Crime

- **Protection from Harassment Act 1997** – covers online harassment and repeated unwanted contact.
- **Public Order Act 1986** & **Racial and Religious Hatred Act 2006** – offences relating to hate speech and inflammatory online content.

Other Relevant Legislation

- **Copyright, Designs and Patents Act 1988** – governs the use of digital media, images, video and online content.
- **Freedom of Information Act 2000** – rights to access information held by public bodies.

- **Human Rights Act 1998** – rights to privacy, expression and protection from discrimination, balanced with safeguarding duties.
- **Prevent Duty (Counter-Terrorism and Security Act 2015)** – responsibilities to prevent radicalisation, including online extremism.