Jessie Younghusband School

e-Safety Policy

Updated March 2026

Review March 2029

Aim

At Jessie Younghusband School we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

- are able to use ICT safely to support their learning in school;
- know how to use a range of ICT equipment safely;
- are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication;
- are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner;
- know what to do if they feel unsafe when it comes to using technology and ICT.

This policy sets out Jessie Younghusband School's commitment to safeguarding children and young people in their use of ICT and modern technologies, both within school and beyond. It aims to empower pupils, staff, and parents to use technology safely and responsibly, in line with statutory safeguarding guidance and West Sussex County Council recommendations.

The Law

Our e-Safety Policy has been written by the school, using advice from WSCC and government guidance. The Policy is part of the school's Strategic Development Plan and related to other policies including Safeguarding and Data Protection policies.

As legislation is often amended and new regulations introduced, the references made in this policy may be superseded. For an up to date list of legislation applying to schools please refer to the Department for Education website at www.education.gov.uk/schools.

This policy is informed by and complies with:

- Keeping Children Safe in Education 2025 (DfE)
- UK Data Protection Act 2018 and GDPR
- West Sussex Safeguarding Children Partnership guidance
- The Education Act 2002 (as amended)
- The Computer Misuse Act 1990 and other relevant legislation.

Our approach addresses the four key areas of online risk:

- Content: exposure to harmful or inappropriate material
- Contact: harmful interactions with others online
- Conduct: risky online behaviour including bullying and sharing explicit images
- Commerce: risks such as online scams and inappropriate advertising.

Roles and Responsibilities

The Headteacher, alongside the e-Safety officer (DHT) will:

- ensure the policy is implemented, communicated and compliance with the policy is monitored;
- ensure staff training in e-Safety is provided and updated annually as part of safeguarding training;
- ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites;

- ensure that all reported incidents of cyber bullying are investigated;
- ensure that appropriate web filtering software is used to protect users from potentially damaging / offensive material.

Teachers and Staff will:

- keep passwords private and only use their own login details, which are stored securely;
- monitor and supervise pupils' internet usage and use of other IT resources;
- adhere to the JYS Acceptable Use of ICT policy;
- promote e-Safety and teach e-Safety units as part of the computing curriculum;
- actively engage in e-Safety training;
- only download attachments / material onto the school system if they are from a trusted source;
- when capturing images, videos or sound clips of children, only use school cameras or recording devices.

It is essential that pupils, parents, carers and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Governors will:

- ensure that the school is implementing this policy effectively;
- adhere to the JYS Acceptable Use of ICT policy when in school;
- have due regard for the importance of e-safety in school.

All staff, including governors and volunteers, will receive safeguarding and child protection training at induction, with annual updates including online safety. Training will cover responsibilities related to filtering, monitoring, and reporting concerns as outlined in KCSIE.

Education

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for ICT at Key Stages 1 to 4 makes it mandatory for children to be taught how to use ICT safely and securely. Together, these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. To support this, the following procedures are in place:

- e-Safety rules are posted in all rooms where computers are used and discussed with pupils regularly;
- pupils are informed that network and Internet use will be monitored, and any misuse of the internet will be appropriately followed up by the e-Safety / IT Leader;
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices

to any new 'e-activities' they encounter. We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

The school will actively teach e-Safety at an age-appropriate level. The school follows a scheme of work for each year group covering:

- what should and shouldn't be shared online;
- password control;
- cyber-bullying (among other topics).

Online safety education is embedded within the computing curriculum and reinforced across the wider curriculum and PSHE. It is tailored to pupils' age and needs, including those with SEND. This education aims to build resilience and empower pupils to recognise and respond to online risks.

We actively engage parents and carers through communication, newsletters, and resources to support safe technology use at home. Parents are informed of the school's e-Safety policy and encouraged to reinforce safe practises

Monitoring safe and secure systems

We use Device Doctors filtered broadband and monitoring software to restrict access to inappropriate content. Any attempts to access unsuitable material are logged and investigated promptly by the e-Safety officer (Headteacher). Antivirus software has been installed on all computers and is to be maintained and updated regularly. We run a cloud-based system which is encrypted and requires 2 factor authentication. Staff passwords should be changed regularly and must be strong passwords or pass phrases. Staff take responsibility for safeguarding confidential data saved to the cloud and this must be via Microsoft, i.e. use of strong passwords. No personal data should be saved to USB / data sticks. Staff with access to the ICT systems containing confidential and personal data are to ensure that such data is properly protected at all times. All staff have remote access to the school cloud (Microsoft 365). This reduces the need for portable data storage and therefore increases security.

Safe use of the Internet and Web Filtering

- all staff and pupils will have access to the internet through the school's network;
- all staff, volunteers who have use of the school's IT equipment, must read and sign the JYS Acceptable Use of ICT policy;
- if a site containing inappropriate material is encountered, children must report it to an adult who will report it to the e-Safety officer to pass to Device Doctors. The alert system we use will flag any inappropriate internet searches and access to pages that breach our guidelines. These will be investigated by the e-safety officer and followed up as required (e.g. possible safeguarding, recorded if needed)
- if an adult finds a site that they consider unsuitable, they should report it to the IT Leader who is responsible for e-Safety in school.
- All e-Safety incidents, including cyberbullying and inappropriate content, will be recorded and managed in line with the school's safeguarding and behaviour policies. Serious concerns will be escalated to the designated safeguarding lead (Headteacher) and external agencies as required.

The use of Email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails. All emails should be professional in nature and staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email.

The school website

The school web site complies with statutory DFE requirements. The school may publish images that include photographs of children pursuing school activities. These will be unnamed and monitored closely by school staff to ensure they are appropriate, in accordance with the school's Data Protection Policy.

Social Networking, Social Media and Personal Publishing (blogging)

The school recognises that it has a duty to help keep children safe when they are accessing such sites at home, and to this end the school will cover such issues within the curriculum. Pupils are not permitted to access social networking sites on school devices. Staff personal mobile devices must not be used for contacting pupils unless authorised by the Headteacher. The school reserves the right to search mobile devices on premises where there is reasonable suspicion of inappropriate content.

Staff private use of social media:

These are all the rules relating to the staff's private use of social media:

- no reference should be made in social media to students / pupils, parents / carers / school staff or issues / situations related to the school (full details of expectations for staff are set out in the Staff Code of Conduct);
- staff should not engage in online discussion on personal matters relating to members of the school community;
- personal opinions should not be attributed to the school;
- security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information;
- teachers should not run social network spaces for student use on a personal basis or open up their own spaces to their students, they should use the schools' preferred system for such communications.

The Use of Cameras, Video and Audio Recording Equipment

Staff may only use the school's photographic or video devices to support school trips and curriculum activities or personal devices that have Teams installed and logged into a school account. This can used as a platform to capture images (as it does not save to the local device). Photos should only be uploaded to the school system. They should never upload images to the internet unless specific arrangements have been agreed with the Headteacher or Deputy Headteacher, nor circulate them in electronic form outside the school. It is never acceptable to use photographic or video devices in changing rooms or toilets.

Personal mobile phones and mobile devices

All pupils must hand mobile phones to the class teacher at the start of the day and are not permitted to carry or use a phone in school. The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring at the direction of the head teacher. They should not be used in front of children other than for educational purposes (e.g. taking a register)

Staff should not use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity unless this has been agreed by the Headteacher to meet a certain situation.

Protecting School Staff

In order to protect school staff, we require that parents do not comment on school issues or staff using social networking sites. Any concerns or complaints should be discussed directly with the school. The school will take action if there is evidence that inappropriate comments about staff have been placed on the internet in a public arena.

Policies

The policies and guidance to help form a safe environment to learn and work in include, but are not limited to:

- the Acceptable Use of ICT Policy JSPC's Internet Filtering Policy;
- photographic images of children guidelines for staff and parents;
- West Sussex Guidance for The Safer Use of the Internet
- JYS Staff Code of Conduct and Staff Handbook

These policies set the boundaries of acceptable use. Hard copies can be found in the staff room and a copy is available on the Teacher Shared portion of the server. They have links with other school policies such as:

- Behaviour Policy;
- Anti-bullying policy;
- Data Protection Policy. (GDPR).

Writing and reviewing the e-Safety Policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.

The Computing co-ordinator has the role of e-Safety officer. The e-Safety officer works closely with the member of staff responsible for Child Protection, which at Jessie Younghusband School is the Headteacher. N.B. The e-Safety officer is not a technical role.

Our e-Safety Policy has been written by the school, building on the West Sussex e-Safety Policy and government guidance. It is shared with all staff and approved by governors.

Learning and teaching at Jessie Younghusband School

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning.

Jessie Younghusband School Internet access has been designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils are taught:

- what kind of Internet use is acceptable - and what is not - and given clear objectives for Internet use.
- the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- how to publish and present information to a wider audience.
- how to evaluate Internet content.
- the importance of cross-checking information before accepting its accuracy.
- to report unpleasant Internet content to the Headteacher, or their class teacher who will share this information with the e-Safety officer, so that a path of action can be agreed.

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Managing Internet access at Jessie Younghusband School: Information System security

School ICT systems security is reviewed regularly.

Virus protection is updated regularly.

Published content and the school website

Pupils' personal details are not to be published on the website.
The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

There are a number of issues to be considered when it comes to publishing pupils' images and work. These include:

- pupils' full names will not be used with their photographs anywhere on the school website or other online space;
- work can only be published with the permission of the pupil and parents/carers;
- parents are clearly informed of the school policy on image taking and publishing in the school's Privacy Notice for Parents, Carers;
- the school filters do not allow access to major social networking sites. Pupils are taught how to use messaging via secure systems, including the school's VLE, which is moderated;
- pupils are advised never to give out personal details of any kind which may identify them, their friends or their location;
- pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils;
- pupils are advised to use nicknames and avatars when using social networking sites outside of school.

Managing Filtering

The school works with Device Doctors, West Sussex County Council and other e-Safety sites to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable online materials, the site must be reported to the e-Safety officer.

Pupils will always work with a supervising teacher when making or answering a video conference call.

Protecting personal data

The school aims to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018.

Authorising Internet access

All staff must read and sign the JYS Acceptable Use of ICT policy before using any school ICT resource.

The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At EYFS and KS1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved software.

Any person not directly employed by the school will be asked to sign the JYS Acceptable Use of ICT Policy before being allowed to access the school's Wi-Fi via a password.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor West Sussex County Council can accept liability for any material accessed, or any consequences of Internet access.

The school will audit ICT use to establish if the e-Safety Policy is adequate and that the implementation of the e-Safety Policy is appropriate and effective.

Handling e-Safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Pupils and parents will be informed of the complaints policy and they will be informed of consequences for pupils misusing the Internet.

Staff and the e-Safety Policy

All staff will be given the School e-Safety Policy and its importance explained.

"West Sussex Guidance for The Safer Use of the Internet by Staff Working with young People" provides more details for adults at school to be aware of in order to ensure everyone is 'e-Safe'.

Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by the Headteacher and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.

The school will ask all new parents to sign the "New Starter Booklet" when they register their child with the school.

The school will maintain a list of e-Safety resources for parents / carers.

External media on portable devices

Staff and children should be aware of the associated risks of connecting devices to networks outside the school, and the possible harm that any downloaded files might bring.