Jessie Younghusband School

e-Safety Policy

Updated October 2018

Review December 2020

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 outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home.

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As legislation is often amended and new regulations introduced, the references made in this policy may be superseded.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.

Roles and Responsibilities

The Headteacher, alongside the e-safety officer (Paul Neaves) 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 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 Acceptable Use Agreement;
- Promote e-Safety and teach e-Safety units as part of the computing curriculum;
- 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 acceptable use agreement when in school;
- Have due regard for the importance of e-safety in school.

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 appropriately followed up;
- 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 and cyber bullying among other topics. e-Safety will also be embedded throughout learning whenever children are using ICT in other lessons.

Monitoring safe and secure systems

Internet access is regulated by JSPC supplied filtered broadband connection which blocks access to unsuitable websites. Antivirus software has been installed on all computers and is to be maintained and updated regularly. Staff passwords should be changed regularly and must be strong passwords. Staff take responsibility for safeguarding confidential data saved to laptops, i.e. use of strong passwords. If personal data has to be saved to other media, e.g. data sticks, it is to be encrypted or strong password protected. Staff with access to the ICT systems containing confidential and personal

data are to ensure that such data is properly protected at all times. Teaching staff have remote access to the school server. This reduces the need for portable data storage and therefore increases security. Remote access is fully password protected.

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 Staff Acceptable Use Agreement;
* If a site containing inappropriate material is encountered, children must report it to an adult who will report it to the Computing lead to pass to JSPC;
* If an adult finds a site that they consider unsuitable they should report it to the Computing lead.

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;
- Images that include pupils will be selected carefully and only used if parents have given permission for such images to be posted on line.

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 will not access social networking sites, e.g. Facebook or Twitter in school. They will be taught about how to stay safe when using such sites at home. School and class blogs are run through the school website and are password protected.

Staff 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;
- 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;
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to 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. 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

- 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.
- Staff are not permitted to 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.

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 Policy (AUP) based on WSCC Guidelines;
- JSPC's Internet Filtering Policy;
- Photographic images of children guidelines for staff and parents;
- West Sussex Guidance for The Safer Use of the Internet by Staff Working with Young People.

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 management policy;
- Anti-bullying policy;
- Staff handbook;
- Code of conduct for staff.

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 (with support from the ICT Technician) has the role of e-Safety Coordinator. The e-Safety Coordinator works closely with the member of staff responsible for Child Protection, which at Jessie Younghusband School is the Headteacher. N.B. The e-Safety Coordinator 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.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.
- Pupils are taught how to evaluate Internet content.
- Pupils are taught the importance of cross-checking information before accepting its accuracy.
- Pupils are taught to report unpleasant Internet content to the Headteacher, or their class teacher who will share this information with the e-Safety Coordinator, 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' details are not available 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:

- Photographs that include pupils will be selected carefully with the permission of parents/guardians;
- 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, both on school and independent electronic repositories, social networking and personal publishing;
- 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 JSPC, 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 Coordinator.

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

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

All staff must read and sign the "Staff Acceptable Use 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 an "Acceptable Use Agreement" before being allowed to access the Internet from the school site.

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 parent /pupil agreement 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.