e-Safety Policy

Date of next policy review	**September 2021**
Name of person responsible for this policy	**Mr Clarke/Mr C. Fulton/SLT**
Other related policies	**ICT, Behaviour and Citizenship, Pastoral Care, Safeguarding**
Issued to	**Staff, governors, parents**
Date of issue	**September 2019**

e–Safety Policy

Purpose

Victoria Primary School believes that the use of ICT in schools brings great benefits. In today's society, children, young people and adults interact with technologies such as mobile phones, tablets, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally, potentially place children, young people and adults in danger.

Our e-Safety policy therefore covers issues relating to pupils, staff, parents and the school community regarding their safe use of the Internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with pupils in Victoria Primary School.

We aim to empower and educate our pupils so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns. All members of staff need to be aware of the importance of good e-Safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. It is crucial that everyone is aware of the offline consequences that online actions can have. We aim to inform and support parents and the school community in helping their children to use ICT effectively and safely at all times.

Benefits of using ICT and the Internet to pupils and the school include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with EA and DE;
- access to learning wherever and whenever convenient.

Definition of terms

ICT – Information Communication Technology
Key Stage 1 – P1 – P4
Key Stage 2 – P5 – P7
EA – Education Authority
DE – Department of Education
C2K – School network managers

Management

Managing Information Systems

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.
ICT security is a complex issue which cannot be dealt with adequately within this document.
Local Area Network (LAN) security issues include:

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Users must take responsibility for their network use.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date.
- Virus protection for the whole network must be installed and current.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

The School's network is managed by C2k/Capita who ensure security and virus protection.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly via C2k/ Capita .
- Personal data sent over the Internet or taken off site should be encrypted.
- Care must be taken with portable media. The media device should be checked by the ICT Coordinator , followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Schools Acceptable Use Policy' before using any school ICT resources.

- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy.
- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

Management of Published content

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.

Management of Pupil work/images

- Images or videos that include pupils will be selected carefully
- Pupils' names will not be used anywhere on the website, particularly in association with photographs unless consent is given.
- Written/verbal permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will also include information pertaining to the use of photographic images of children in the Safeguarding policy.
- The school will request GDPR consent from each parent in relation to the publishing of personal information. The retention period is clearly highlighted on the GDPR consent form.

Protection of personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and further General Data Protection Regulation Legislation.

Teaching, Learning and ICT

Pupils

Consideration must be given as to the curriculum place for teaching e–Safety.

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils will be educated in the effective use of the ICT in research, including the 5 'e' skills.
- Pupils will learn digital literacy skills and to refine their own publishing and communications with others.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- e–Safety will be included in the PDMU, Citizenship and/or ICT schemes of work covering both safe school and home use.
- To protect all pupils, the school will implement Acceptable Use Policies.
- Pupils will have opportunity to learn about e–Safety each September (and other appropriate times) to improve knowledge and reinforce importance of safe and responsible internet/ICT use amongst pupils.
- Pupils will learn responsible and safe use before Internet access.
- All pupils will be informed that network and Internet use will be monitored by school/C2K
- Pupils in P5 in P7 will have opportunity to participate in Key Stage transition e–Safety learning
- e-Safety rules or copies of the Pupil Acceptable Use Poster will be posted in all rooms with Internet access.
- Vunerable pupils will receive specific attention in relation to Particular attention to e-Safety as required.
- Pupils will have weekly access to iPads/computers/cameras/internet (dependent upon lessons and Key Stage)
- At Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information

received via the Internet, email or text message requires even better information handling and digital literacy skills. In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. A whole curriculum approach may be required.
Researching potentially emotive themes such as the Holocaust, animal testing, nuclear energy etc provide an opportunity for pupils to develop skills in evaluating Internet content. For example researching the Holocaust will undoubtedly lead to Holocaust denial sites which teachers must be aware of. Therefore:

- Pupils will learn to be critically aware of the materials they read and how to validate information before accepting its accuracy.
- Pupils will develop their use of age-appropriate tools to research Internet content.

Teaching, Learning and ICT

Staff

- The e–Safety scheme will be taught across the school each September (and other appropriate times) to raise the awareness and importance of safe and responsible internet/ICT use amongst pupils.
- To protect all pupils and staff, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The school's Internet access will be designed to enhance and extend education. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.
- The School will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- Staff will only use official school provided email accounts to communicate with parents/carers or external professional agencies.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- Staff should not use personal email accounts during school hours or for professional purposes.

Responsible Use of ICT in the community

Home school Partnership

- Parents' attention will be drawn to the school e–Safety Policy in information leaflets, parent evenings or workshops, newsletters, the school prospectus and on the school website.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days.
- Parents will be requested to sign an e–Safety/Internet home school agreement as part of the Home School Agreement.
- Parents will be given opportunity to give written permission for the school to use their child's photograph both in school and on the school website.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.
- Interested parents will be referred to organisations listed in the appendix for further information.

Procedure

Risk Assessment

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor the Education Authority can accept liability for the material accessed, or any consequences resulting from Internet use.
- 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.

How will the school respond to any incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-Safety concerns.
- The Principal and Designated Child Protection Teacher/team will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety incidents in accordance with the school citizenship and behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school SLT will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Gateway Team or Child protection team at E.A. and if necessary escalate the concern to the PSNI.
- If the school is unsure how to proceed with any incidents of concern, then the incident should be reported to Schools' Branch E.A.

e–Safety complaints regarding use of the internet/ICT in school

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.

- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

Mobile phones and personal devices

- Pupils are not allowed mobile phones or other electronic devises in school at any time for any reason.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- If a pupil is a victim to the abusive or inappropriate messages being sent via mobile phones, as a school, we will provide the pupil with support as per our pastoral care policy, with our pastoral lead, Miss J. Minnis, taking a role in supporting the pupil.
- School will contact a pupil's parents or guardians if required.

Staff / Volunteer Use of Personal Devices

- **Staff / Volunteer** are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- **Staff / Volunteer** should not use personal devices such as mobile phones, tablets or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

e–Safety complaints regarding use of the internet/ICT out of school

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the Principal.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with the school to resolve issues.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- **The school cannot be held responsible for matters pertaining to e-safety that originate outside the school times and school environment.**
- The school cannot share information in any manner that would contravene data protection laws.
- No pupil under 13 should be accessing or using social networking sites.

Cyberbullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyberbullying (along with all other forms of bullying) of any member of the school community should not be tolerated. Full details are set out in the school's policy on anti-bullying and citizenship and behaviour policies.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- No pupil under 13 should be accessing or using social networking sites.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying that directly affect pupils' learning in the school environment.

- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- **<u>The school cannot be held responsible for matters pertaining to e- safety that originate outside the school times and school environment.</u>**
- The school will contact the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.
- Sanctions for those involved in cyberbullying committed in school may include:
    - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.
    - Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
    - Parent/carers of pupils will be informed.
    - The Police will be contacted if a criminal offence is suspected.

Appendix 1

e-Safety Contacts and References

Victoria primary School: www.victoriaprimary.org.uk

www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
C2k/Capita: www.C2kni.net

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com