Strandtown Primary School

Use of Internet
&
Digital Technologies Policy Incorporating E-Safety

Updated	Review Date
September 2022	September 2023

Rationale

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The school's safe use of Internet and Digital Technology policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum and Child Protection.

This E-Safety policy was approved by the Board of Governors on:	
The implementation of this E-Safety policy will be monitored by the:	E-Safety Officer Safeguarding Team SLT
Monitoring will take place at regular intervals:	Annually
The Board of Governors will receive a report on the implementation of the E-Safety policy generated by the monitoring group (which will include anonymous details of E-Safety incidents) at regular intervals:	Annually
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to E-Safety or incidents that have taken place. The next anticipated review date will be:	December June 2022
Should serious E-Safety incidents take place, the following external persons / agencies should be informed:	Child Protection Agency / PSNI

Values and Mission Statement

At Strandtown Primary School our vision is to inspire a positive and happy environment, using e-safety education to raise the awareness of the issues and risks and provide strategies for dealing with them and those who work with them, encouraging them how to use digital technology safely and responsibly.

Our vision encompasses the following aims:

- E-safety education will be embedded into everyday school life.
- To provide opportunities to enable all staff and pupils to be confident and responsible users of digital technology.
- To use ICT to develop an online community, sharing ideas and resources between pupils, staff, parents, Board of Governors, other schools and the wider community.

Aims

Across the curriculum at a level appropriate to their ability pupils will be empowered to use the internet and different technologies in a safe and positive way.

Adults will be supported in safeguarding and protecting pupils from the potential risks of online and mobile communication.

Methodology

Our E-safety curriculum is designed to help children keep themselves safe online by developing skills in identifying and avoiding risk, learning how to best protect themselves and their friends and knowing how to get support and report abuse if they do encounter difficulties.

Curriculum Leadership

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school.

Board of Governors

Governors are responsible for the approval of the E-Safety Policy. Governors will be provided with regular information about E-Safety incidents. The Governors will:

- have regular meetings with the school safeguarding team.
- monitor of E-Safety incident logs (Securus / E-safety incident report forms)

Principal

- The Principal has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the safeguarding team.
- The Principal and members of the Safeguarding Team 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 Principal is responsible for ensuring that the Safeguarding Team and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the Safeguarding team.

E-Safety Officer

- Is part of the Safeguarding Team.
- Takes day to day responsibility for E-Safety issues and have 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.
- Provides training and advice for staff.
- Liaises with the relevant body.
- Receives reports of E-Safety incidents (Securus/ E-safety incident report form) and creates a log of incidents to inform future E-Safety developments.
- Meets regularly with Senior Leadership Team to discuss current issues, review incident logs and filtering changes.
- Attends relevant meetings of Governors.
- Sets relevant targets in line with the school development plan.
- Uses the 360 Safe platform to monitor and evaluate the school's e-safety progress and compliance.

<u>The E-safety Officer is responsible for ensuring:</u>

- that the school meets required E-Safety technical requirements**.**
- filtering settings are differentiated to suit users' needs.
- any changes to filtering settings are recorded.
- 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.
- that the use of the network, internet and Virtual Learning Environment is regularly monitored in order that any misuse / attempted misuse can be reported to the ICT Coordinator. Pupil and staff use is monitored through the Mosyle Manager MDM and Securus platform.

- that e-safety in school is regularly monitored and evaluated using action plans, reports and relevant 360 Safe online evaluation data.

360 Degree Safe

Strandtown Primary School use the 360 degree safe self-review tool to evaluate and enhance our online safety policy and practice. The online program provides:

- Information that can influence the production or review of online safety policies and develop good practice.
- A process for identifying strengths and weaknesses.
- Opportunities for commitment and involvement from the whole school.

Staff

- All staff will sign an Acceptable Use Agreement annually, and on appointment.
- They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices.
- They report any suspected misuse or problem to the ICT Coordinator.
- Staff must be aware of dangers to themselves in monitoring ICT use, for instance in viewing inappropriate images to investigate their source. Any allegation of inappropriate behaviour must be reported to senior management.
- All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems.
- Ensure E-Safety issues are embedded in all aspects of the curriculum and other activities.
- Ensure pupils understand and follow the E-Safety and acceptable use policies.
- Discuss the importance of research skills and the need to avoid plagiarism and uphold copyright regulations.
- 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.
- In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Child Protection Teachers

The designated child protection teachers 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
- Online Bullying

Safeguarding Team

The safeguarding team has wide representation from the school community, with responsibility for issues regarding E-Safety and the monitoring of the E-Safety policy including the impact of initiatives. The group will also be responsible for regular reporting to the Board of Governors.

Members of the Safeguarding team will assist the E-Safety Officer with:

- The production / review / monitoring of the school E-Safety policy.
- Monitoring network / internet / incident logs.
- Consulting stakeholders – including parents / carers and the pupils about the E-Safety provision.
- Monitoring improvement actions identified through use of the 360 Safe self-review tool.

Pupils

- All pupils will sign an Acceptable Use Policy and use the school systems in accordance with this.
- Staff reserve the right to enter any pupil's folder.
- Pupils must not use the Internet for unapproved purposes.
- Pupils should be discouraged from bringing mobile phones, hand-held gaming consoles with downloadable capabilities or mobile technology to schools on the grounds that they:
    - are valuable and may be lost or stolen.
    - are capable of storing images that are inappropriate
    - do not have the internet filters appropriate for school.
- Will be expected to know and understand rules on the use of mobile devices and digital cameras. They should also know and understand code of conduct on the taking / use of images and on cyber-bullying.
- Mobile phones will not be switched on during school time.
- Have discussed the importance of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good E-Safety practice when using digital technologies 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

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' evenings, newsletters, letters and website. 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.
- their children's personal devices in the school.
- Parents should be aware that the access to the Internet provided to staff and pupils in school has limiting security features.
- Parents should be aware that the use of the Internet in school is closely monitored by staff.
- Parents should be aware that there will be no use of the Internet without the supervision of staff and that this will be in full view of others, e.g. the classroom or the library

- Parents should, in co-operation with staff, make pupils aware of the rules and expectations within this document.
- Parents should be aware that no photographs of pupils will be available online without parents giving their permission.
- Parents should discourage pupils from using personal mobile technology within school.

Community Users

Community Users who access school systems as part of the wider school provision will be expected to sign a Volunteer User Agreement before being provided with access to the school systems.

E-Safety Education

Education - Pupils

Pupils need to learn safety rules in a way that does not frighten them and which gives them confidence to know what to do in certain situations. E-Safety should be a focus in all areas of the curriculum.

- A planned E-Safety curriculum should be provided as part of PDMU and ICT lessons. It should be regularly revisited.
- Key E-Safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils need to understand that certain rules will change and develop as they get older.
- Pupils need to learn how to apply strategies that will help them to avoid certain risks.
- Pupils need to understand that E-Safety rules given to them must be followed.

Cross Curricular Skills

E-safety will be taught and reinforced through all areas of the curriculum.

Promoting Thinking Skills and Personal Capabilities

At the core of our vision for E-safety is that we are aiming to encourage pupils to think critically and apply this to real life situations. Our methodology also aims to promote collaborative learning. The teaching of Thinking Skills and Personal Capabilities is inextricably intertwined to the goals of the E-safety policy.

Education - Parents/Carers

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours.

The school will therefore seek to provide information and awareness to parents and carers through:

- letters, newsletters, website, parent mail, school app
- parent / carer support sessions
- E-Safety themed week (Safer Internet day)
- reference to the relevant web sites / publications

Education & Training - Staff/Volunteers

It is essential that all staff receive E-Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- all new staff should receive E-Safety training as part of their induction programme, ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements.
- this E-Safety policy and its updates will be presented to and discussed by staff.
- the Safeguarding team will provide advice / guidance / training to individuals as required.

Introducing the Safe Use of Internet and Digital Technologies to:

Pupils

- Safe use of Internet rules will be discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored. (E.g. Securus)
- Instruction in responsible and safe use should precede Internet access.

Staff

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

Parents

- Parents' attention will be drawn to the School E-Safety policy.

Technical – infrastructure / equipment, filtering and monitoring

- The school will work with C2k and the Internet Service Provider to ensure that the school meets recommended technical requirements.
- Servers must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers.
- There will be regular reviews of the safety and security of school technical systems.
- The ICT Coordinator is responsible for ensuring that software licences purchased by the school match the number of software installations.
- Internet access is filtered for all users.
- The E-safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- If staff or pupils discover an unsuitable site, it must be reported to their teacher or designated teacher for child protection.
- All users will be provided with a username and password. Users are responsible for the security of their user name and password.
- All users are made aware that the school may check their computer files and may monitor the Internet sites visited.
- Guests requiring temporary access will be given a guest username and password and will have to sign an Acceptable Use Agreement before gaining access to the network.
- School devices that may be used out of school should only be used by a designated user for school related purposes.
- Staff should be aware that downloading executable files can corrupt the system.

Use of School Owned Technologies Outside School

When school owned technology is taken off the premises it should only be used for professional purposes. All data and information is stored on cloud-based software. This means it can be securely accessed from any location removing the need to carry data and files on insecure data pens and portable devices. Staff should refrain from saving to the local drive and confidential files should be uploaded to MySchool. Any confidential files saved locally should be deleted.

Managing Emerging Technologies

Emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia.

- Emerging technologies will be examined for educational benefit before being implemented by the school.
- The school has a set of clear expectations and responsibilities for all users.
- The school adheres to the Data Protection Act principles.
- All users are provided with and accept the Acceptable Use Agreement.
- All network systems are secure and access for users is differentiated.
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises.
- All users will use their username and password and keep this safe.
- Training is undertaken for all staff.
- Regular audits and monitoring of usage will take place to ensure compliance.
- Any device loss, theft, change of ownership of the device will be reported.

Making and Storing Digital and Video Images

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 recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- 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.
- Staff members should where possible use school equipment.
- 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.
- *Staff must not use personal devices to record images of children or colleagues. Any images taken on school owned devices must not be taken off site without the prior consent of the*

Vice Principal or Principal. On the rare occasion that Staff are outside of school on a residential trip or sporting activity, they are permitted to take images, with the understanding that they are uploaded to the school system and deleted before the end of the day.

Digital and Video Images of pupils on school websites

Including images of pupils on the school's website or on Class Dojo can be motivating for the pupils involved and provides good opportunities to celebrate and promote the work of the school.

- Parental consent will be requested to cover use of such photographs throughout the school year before using images of pupils on the website or elsewhere.
- Where possible, group photos will be used rather than full-face photos of individual children.
- Names and images will be kept separate on the school website.

Protecting Professional Identity

When communicating with parents and members of the wider community staff should only use school systems, e.g. school e-mail, Class Dojo, our school website and phone in school office. If a personal mobile device must be used for communication with parents, the user must ensure that personal phone numbers are withheld. All communications should be professional in nature.

Social Media

School staff should ensure that:

- No reference should be made in social media to pupils, parents / carer's 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 Strandtown Primary School or local authority.
- They do **not** correspond with pupils through social networking sites or add them as 'friends' or 'followers.'
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
  - *Further information is available via Social Media Policy.*

Social Media – Responsible Use

Within school we have an E-safety curriculum which ensures that;

- Children are aware of the legal ages for social networking sites.
- Children are aware of appropriate online behaviour.
- Children are equipped to be responsible users.
- Children are aware that all online activity can be monitored.
- Children have an understanding of privacy settings and how important it is to use them.
- Children understand what to do if they are worried about anything they have seen online.

Mobile Devices

We recognise that access to mobile phones by children has become a useful tool for families to keep in contact with each other in case of emergency on the way to and from school. However, during school hours' children and parents can access each other through the school office therefore, all mobile phones must be switched off in school and stored in school bags.

When using mobile devices such as iPads pupils and staff must adhere to the guidelines stated in Acceptable Use Policies. Digital and video images taken on mobile devices must be deleted as soon as they have been used.

Respecting Children's Rights and Equality of Opportunity

Strandtown Primary School aims to empower children through ICT and enhance their protection. It will contribute to the realisation of the rights of the child to participation, education, and protection from abuse, violence and exploitation in the digital world by addressing the following articles from a Summary of the UN Convention on the Rights of the Child;

- Article 3 – best interests of the child.
- Article 12 – respect for the views of the child.
- Article 13 – freedom of expression.
- Article 17 – access to information from the media.
- Article 36 – other forms of exploitation.

Strandtown Primary School's ICT facilities are available for use by all pupils and staff. All children are given access to ICT regardless of gender, race, physical or sensory disability.

E-Safety and Pupil Support

Children receiving pupil support (SEN) can use the digital technologies in educational, creative, empowering and fun ways. However, they may be particularly vulnerable to E-safety risks. In collaboration with the Pupil Support Coordinator class teachers will develop strategies for safe use of digital technologies for children with SEN.

Professional Development

The school is committed to cater for teachers' professional development needs within the area of e-safety. These include the following key elements:

- A clear and user-friendly E-safety policy and curriculum overview.
- An appropriate and varied range of resources.
- The support and encouragement of the safeguarding team.
- Ongoing training and professional development as required.

The Monitoring and Evaluation of the E-Safety Policy

The school will monitor the impact of this policy using:

- logs of reported incidents
- pupil focus groups
- feedback from staff

Review Cycle of Policy

The E-safety policy will be reviewed and updated annually. A copy of the policy will be available in the school office on request and on the school website.

User Actions – Unsuitable / Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)		X				
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X	X		
File sharing				X		
Use of social media (School use)				X		
Use of messaging apps				X		
Use of video broadcasting eg Youtube				X		

Handling E-Safety Complaints

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

- Parents, teachers and pupils should know how to submit a complaint.
- A range of sanctions will be required when rules are breached, linked to the school's disciplinary policy.

Illegal Incidents

- If there is any other suspected illegal activity, report to the Safeguarding team.
- If the school identifies a suspect computer (containing for instance indecent images or offences concerning child protection), it should **not** be used or viewed. Schools should isolate any devices concerned and take advice from local police.
- **In some circumstances such interference may also constitute a criminal offence. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or Safeguarding team.**

After a major or minor incident, a comprehensive debriefing should occur to review school policy and procedures, to make and monitor any necessary changes and to maximise what can be learnt.

- Complaints of Internet misuse will be dealt with by the Safeguarding team.
- Any complaint about staff misuse must be referred to the designated teachers for child protection.
- 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 procedure.

School Actions & Sanctions - Pupils

It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Incidents:	Refer to class teacher	Refer to Head of Year	Refer to Safeguarding team	Consider referral to Police/outside agencies	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction s
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X							X	
Unauthorised use of social media / messaging apps / personal email	X				X			X	
Unauthorised downloading or uploading of files	X				X			X	
Allowing others to access school / academy network by sharing username and passwords	X							X	
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X							X	
Attempting to access or accessing the school / academy network, using the account of a member of staff			X						X
Corrupting or destroying the data of other users			X						X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						X
Continued infringements of the above, following previous warnings or sanctions			X			X	X		
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X			X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident			X			X			
Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X		
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X					X	

School Actions & Sanctions - Staff

Incidents:	Refer to Safeguarding team	Refer to Principal	Refer to C2K	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X					X		
Unauthorised downloading or uploading of files	X					X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X					X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules	X	X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X						
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						
Actions which could compromise the staff member's professional standing	X	X						
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy	X	X						
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X			
Breaching copyright or licensing regulations	X	X						
Continued infringements of the above, following previous warnings or sanctions	X	X						

Addendum

- Network administrator reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibility – they will respect the right to privacy whenever possible

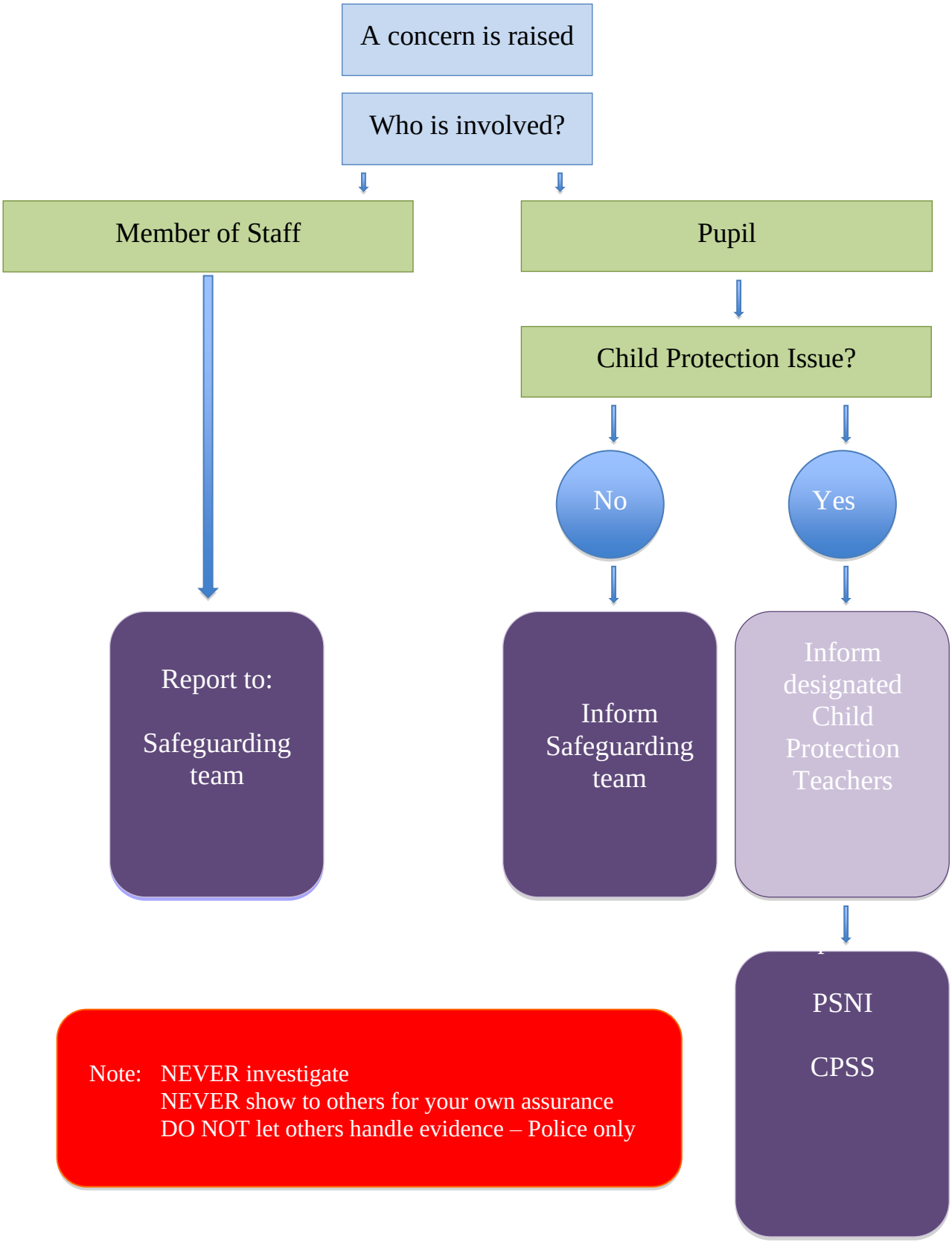
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor C2k can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT provision to establish if the E-Safety policy is adequate and that its implementation is effective.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

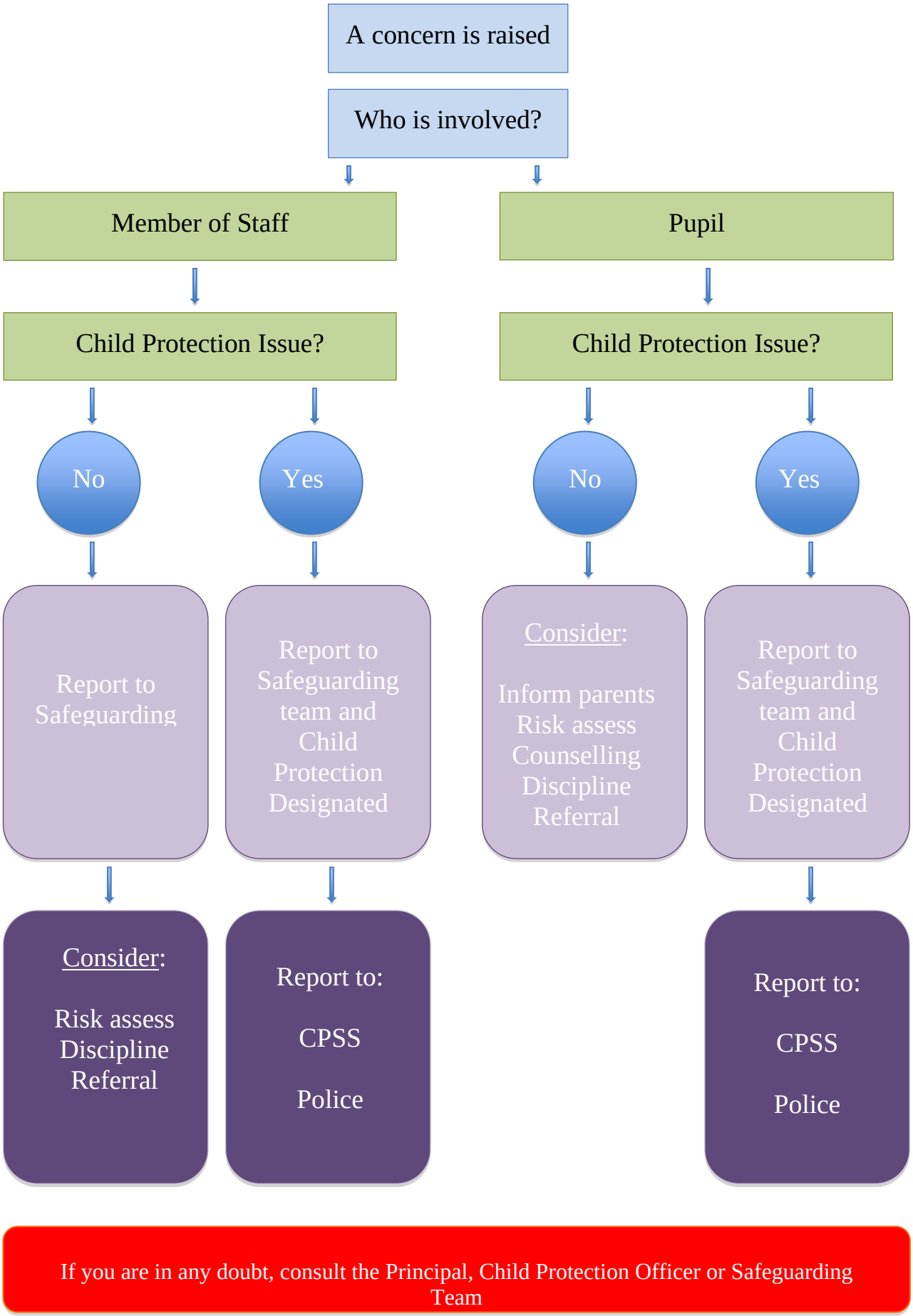
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the *school* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Inappropriate Activity Flowchart



Pupil User Agreement

This Acceptable Use Agreement is intended to ensure that pupils will be responsible users and stay safe while using the internet and other digital technologies for educational use.

- I will access the system with my own username and password which I will keep safe and secure;
- I will not access other people's files;
- I will only use the computers and tablet devices for school work and homework;
- I will not bring in data pens from outside school unless I have been given permission;
- I will ask permission from a member of staff before using the Internet;
- I will only e-mail or message people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent or carer has given permission;
- I will follow the rules and guidelines that my teacher has discussed with the class.
- I will not open e-mails or messages sent by anyone we don't know;
- I will report any unpleasant material or messages sent to me.
- I will only use search engines in the presence of a teacher or another adult in school;
- I will immediately close any webpage I am not sure about;
- I will not use Internet chat rooms or social media accounts.

- I understand that the school may check my computer/device files and may monitor the Internet sites I visit;
- I understand that irresponsible use may result in the loss of network or Internet access.
- I understand that all personal mobile /camera phones must be switched off during school;
- I understand that if using information from the Internet I must include the web address.

Signed:_____ Date:_____

Strandtown Primary School

Safe and Effective Use of the Internet

Agreement & Consent Form

All pupils use computer facilities including Internet access as an essential part of learning, as required by the Northern Ireland Curriculum. Both pupils and their parents/carers are asked to read the rules and sign to show that these have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

- I have read and I understand the Rules for Safe Use of Internet.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Internet Access

I have read and understood the school E-Safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Signed:	***Date:***

Please print name:

Please complete, sign and return to school.

Strandtown Primary School

Staff/Volunteer Information Systems Code of Practice

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's 'Safe Use of Internet and Digital Technologies' policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the principal.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school ICT Coordinator or the Designated Child Protection Teacher.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I understand that staff members may use personal digital devices on field trips; any images should be appropriately transferred back to a centralised area in the staff public folder and deleted that day.
- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I will adhere to Use of Social Media guidelines as set out in Use of Internet and Digital Technologies Policy/ Social Media Policy.
- The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …… Capitals: …… Date: ……