

Glenann Primary School



E-Safety Policy

September 2025

Schedule for Developing, Monitoring and Reviewing Policy

The implementation of this E-Safety policy will be monitored by: The E-Safety Policy has been developed by the staff of Glenann Primary School, under the leadership of the Acting Principals (Mrs Bailey and Miss Loughrey) and the ICT Co-ordinator Miss Loughrey.

Monitoring and Reviewing: Annually, and if required, following a breach of safety.

The Board of Governors will receive regular reports on E-Safety including anonymous details of E-Safety incidents: This will be in conjunction with the Child Protection Report given to the Board of Governors.

Should serious E-Safety incidents take place, the following external persons or agencies should be informed: Police Service for NI (PSNI), Chair of Board of Governors, Education Authority (EA) and Council for Catholic Maintained Schools (CCMS).

Introduction

In Glenann Primary School we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. Staff in Glenann Primary School provide pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

Through the Acceptable Use of the Internet and Digital Technologies in schools the Department of Education (DENI) state that:

“Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools.”

Rationale

“It is essential that pupils and adults are kept safe online whilst in school and on school-organised activities. Schools have a responsibility to ensure that there is a reduced risk of pupils accessing harmful and inappropriate digital content. Schools should be energetic in teaching pupils how to act responsibly and keep themselves safe in the digital world and as a result pupils should have a clear understanding of online safety issues and be able to demonstrate what a positive digital footprint might look like for themselves.”

(DENI Online Safety, Circular number 2016/27)

It is the responsibility of the school’s staff, governors and parents to mitigate risk through reasonable planning and actions. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

The school must demonstrate that it has provided the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks. The E-Safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people, and their parents/carers, to be responsible users and stay safe while using the Internet and other communications technologies for education, personal and recreational use.

Scope of the Policy

This policy applies to all members of the Glenann Primary School community, who have access to, and are users of the school ICT system, both in and out of the school building. In relation to incidents that occur during school hours, we will work with parents, staff and pupils to ensure the E-Safety of all involved, apply sanctions as appropriate and review procedures.

In relation to E-Safety incidents that occur outside of school hours, staff in Glenann Primary School will work with pupils and parents to keep all pupils safe and offer educative support where appropriate. E-Safety outside school hours is primarily the responsibility of the parents. If inappropriate activity occurs outside school hours with the intention of having a negative effect on any member of the Glenann PS community, and this is brought to our attention, then we will liaise with parents as to an appropriate way forward. Any issues that arise inside school, as a result of E-Safety incidents outside of the school, will be dealt with in accordance with our school policies (Safeguarding and Child Protection, Anti-Bullying, Positive Behaviour, Acceptable Use of the Internet and Digital Technologies and Online Safety).

Risk Assessment

“Children and young people have a right to be protected and educated. The report (‘An exploration of e-safety messages to young people, parents and practitioners in Northern Ireland’) highlights the requirement to take appropriate preventative action to protect children and minimise the associated risks around online safety.”

(DENI Online Safety, Circular number 2016/27)

These risks have been defined under four categories.

Content risks: The child or young person is exposed to harmful materials.

Contact risks: The child or young person participates in adult-initiated online activity and/or is at risk of grooming.

Conduct risks: The child or young person is a perpetrator or subject to bullying behaviour in peer-to-peer exchange and/or is at risk of bullying, entrapment and/or blackmail.

Commercial risks: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs/fraud.

These categories have been used to perform a risk assessment (Appendix 1) on the technologies within Glenann Primary School to ensure that everyone is fully aware of and can mitigate the potential risks involved in their use. Pupils need to know how to cope if they come across inappropriate material or situations online. Our risk assessment informs the teaching and learning and develops best practice within the whole school community.

Roles and Responsibilities

At Glenann Primary School we understand that E-Safety must be approached as a whole school. Every member of staff and all the children play an important role in ensuring our school is a safe place to enjoy digital technologies and use them to their full capacity.

Board of Governors

The Board of Governors are responsible for the approval of the E-Safety Policy. It will also be reviewed and monitored by the Safeguarding Team, who meet on a regular basis to discuss new information and developments in relation to Child Protection, Safeguarding and E-Safety.

The 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 ICT Co-ordinator/C2K Manager.

The principal and ICT Co-ordinator will be kept informed about E-Safety incidents.

The principal (the Designated Teacher for Child Protection) will deal with any serious E-Safety allegation being made against a member of staff.

ICT Co-ordinator – Miss Loughrey

The ICT Co-ordinator will take day to day responsibility for E-Safety issues and have a leading role in establishing and reviewing the school's policies and documents.

The ICT Co-ordinator is responsible for:

- keeping up-to-date with new developments and attending any relevant courses in E-Safety;
- disseminating any new developments to all staff;
- ensuring all staff are trained in the procedures and agreed school practice for delivering the E-Safety Policy;
- ensuring there is clear guidance in place for reporting E-Safety incidents to the appropriate body or people;
- keeping a record of any E-Safety incidents which may arise; and
- reporting any relevant incidents to the Safeguarding Team or C2K.

Network / C2K Manager – Miss Loughrey

The Network Manager will monitor that C2K E-Safety measures, as recommended by DENI, are working efficiently within the school.

- The day to day running and maintenance of the school system including updating and maintaining password retrieval and security.
- Assigning temporary usernames and passwords with restricted access to students training in the school.
- Liaising with C2K to ensure the school system is running as it should.
- Setting up agreed access to various levels of Internet filtering or connection of own devices to the school system.

Designated Teacher for Child Protection/Deputy Designated Teacher for Child Protection

The Designated Teacher for Child Protection, Mrs Bailey, and the Deputy Designated Teacher for Child Protection, Miss Loughrey, will be trained in E-Safety issues by the Education Authority and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate online contact with adults/strangers;

- potential or actual incidents of grooming; and
- cyber-bullying.

Teaching Staff

The teaching staff should:

- familiarise themselves with the agreed E-Safety Policy;
- read, understand and sign the Acceptable Use of the Internet and Digital Technologies Policy;
- maintain and monitor own digital profile and ensure any digital communication with pupils (past or present), parents/guardians are on a strict professional basis;
- deliver an agreed set of lessons on E-Safety and digital literacy to their class;
- regularly remind pupils about the importance of E-Safety, reporting procedures and keeping a good digital profile;
- report any suspected misuse or problem to the principal, ICT Co-ordinator/C2K manager and if appropriate ensure this information is passed onto C2K or the Safeguarding and Child Protection Team;
- monitor the use of any digital technologies in their class; and
- keep a secure record of children's usernames and passwords to support children in their class who may forget their passwords.

Non-Teaching Staff and Students

All non-teaching staff and students should:

- maintain and monitor own digital profile and ensure any digital communication with pupils (past or present), parents/guardians are on a strictly professional basis;
- report any suspected misuse or problem to the principal, ICT Co-ordinator/C2K manager and if appropriate ensure this information is passed onto C2K or the Safeguarding and Child Protection Team;
- familiarise themselves with the agreed E-Safety policy; and
- read, understand and give consent to the acceptable use policy.

Pupils

Pupils are responsible for ensuring that:

- they use the school ICT system in accordance with the Pupil Acceptable Use Policy which they will be expected to sign before being given access to school's system;
- they have a good understanding of research skills and the need to avoid plagiarism;
- they understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- they know and understand school guidelines on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand the school's position on the taking / use of images and on cyber-bullying;
- they keep their passwords safe and only using the school system for work set by or agreed by their teacher; and
- they 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 guidelines are good practice and should be adhered to out of school.

Parents / Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the Internet and electronic communication devices in an appropriate way and to support the E-Safety policy outlined by the school.

Parents/carers should ensure that they follow the school guidelines with reference to:

- the use of digital devices and bringing them to school;
- digital and video images taken at school events;
- promoting safe and responsible behaviour by monitoring their children's access to digital devices; and
- encouraging their child to keep a good digital profile and report any behaviour they feel is unsuitable or makes them feel uncomfortable in any way.

Glenann PS will continue to support parents/guardians with this by providing on-line help sheets and websites they can refer to for advice.

Education and Training

Board of Governors and Safeguarding Team

The Board of Governors are kept up-to-date with new developments and EA Online Training will be accessible to all Governors. The Safeguarding Team meet as required to discuss new developments in the areas of E-Safety and Child Protection.

Professional Development for Teaching and Support Staff

Training will be offered as follows:

- all new staff will receive E-Safety training as part of the Induction Programme, ensuring that they fully understand the school E-Safety Policy and Acceptable Use of the Internet and Digital Technologies Policy;
- training in E-Safety will be supported within the PRSD or EPD process and where members of staff have identified a need;
- E-Safety training will be made available to staff as an integral element of CPD;
- staff will be made aware of the importance of filtering systems through the E-Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system; and
- this E-Safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days.

E-Safety Education for Pupils

E-Safety education for students will be provided in the following ways:

- annual participation in Safer Internet Day and Anti-Bullying Week;
- a planned E-Safety programme will be provided as part of ICT/PDMU/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Safer Schools NI App, Safer Internet Day, NSPCC, Childnet, Child Exploitation and Online Protection (CEOP) resources and other recommended resources will be used as a teaching tool;

- robust monitoring of resources and workshops by teaching staff to ensure the information shared by external agencies is appropriate and in line with the Glenann PS E-Safety Policy;
- pupils will be taught in all relevant lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information and to respect Copyright when using material accessed on the Internet;
- pupils will be helped to understand the need for the student Acceptable Use of the Internet and Digital Technologies Policy and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside school;
- where pupils are allowed to search the Internet, staff should be vigilant in monitoring the content of the websites the pupil visit; and
- pupils will be made aware of the importance of filtering systems through the E-Safety education programme.

Parents

Parents and carers have an essential role in the education of their children and in the monitoring and regulation of the children's online behaviours. We use the Glenann PS website and Glenann PS Facebook account to showcase children's participation in Safer Internet lessons and provide access to updated or applicable information with regards to specific guidelines and advice from other agencies.

Current Practice

Communication

The official school email service may be regarded as safe and secure. Email communications with Glenann PS staff, EA, DENI, staff in another school or outside agencies are conducted through the following school email system '@c2kni.net'. Communications with parents are conducted through the Glenann PS School App or the school email system. BCC (Blind Carbon Copy) is used to ensure personal email addresses are not shared. Personal email addresses should not be used.

Users must immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Staff are informed that any digital communication between staff or parents/carers must be professional in tone and content. When emailing, as part of curriculum studies, staff should CC any communication to pupils to another member of staff.

Personal information should not be posted on the official Glenann PS Website or Facebook page and only official email addresses should be used to identify members of staff.

Social Networking

At present, the school endeavours to deny access to social networking sites to pupils during school hours. Where VLE's are used as a form of communication between pupils from Glenann PS and pupils in other schools or with external agencies to achieve the aims of the NI Curriculum, these will be closely monitored by teachers and support staff. Glenann PS has an official school website and operates an official Facebook account. These are used to ensure the school community has up-to-date information about forthcoming events, to provide updates and to communicate recent news. Parental/carer permission for use of digital photographs or video involving their child is obtained through a Data Collection Form at the beginning of the school year. The principal holds responsibility for photographs posted on Facebook. Pupils' full names or personal information will not be posted. Teachers adhere to school policy for photographs and videos shared via the school website. Through the Acceptable Use of the Internet and Digital Technologies Policy, staff agree to adhere to the social networking/communication guidance provided by the school. Staff receive guidance in the appropriate use of social networking in their private life.

Pupils' Use of Personal Devices

Glenann PS does not permit pupils to use mobile phones in the school. The school accepts that there may be circumstances in which a parent wishes their child to have a mobile phone, for example during a residential. These devices will be held by staff and given to pupils to make communication with their parents at an agreed time. If a parent deems it a necessity for a child to bring a mobile phone to school, the mobile phone will be placed in the principal's office on arrival. If a mobile phone is discovered, it will be kept by the principal in a locked safe place until the end of the school day, when it will be returned to the pupil.

Staff Use of Personal Devices

Staff should not use personally owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use school-provided equipment for this purpose. Where staff members are required to use their mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting parents, then they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

By arrangement with the principal, staff may on occasions have use of their phone during class time. This will be arranged on a case-by-case basis and at the discretion of the principal.

CCTV

We have CCTV in the school as part of our site surveillance for staff and pupil safety. The CCTV system records 24 hours per day, 7 days per week. Images will be recorded and are automatically retained on the system for 23 weeks, unless the school is required by law to retain them longer and/or it is necessary for the school to retain any footage as part of the investigation of an incident. In the case of the latter the relevant footage will be stored securely until it is no longer required for the purpose for which it was retained. Otherwise, the CCTV System will automatically delete the images it records after 23 weeks. We will not

reveal any recordings without permission, except were disclosed to the Police as part of a criminal investigation.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents and pupils need to be aware of the risks associated with taking digital images and sharing on the Internet.

When using digital images, members of staff inform and educate pupils about the risks associated with taking, using, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the Internet e.g. social networking sites.

As each teacher has access to a staff iPad, teachers, children or other members of staff are not permitted to use their own devices to take photos of the children. Images and videos taken on staff iPads will be transferred to a centralised area which can only be accessed by teachers. Images and videos will then be deleted from iPads.

- The school will comply with the Data Protection Act by requesting parents' permission for use of digital photographs or video involving their child at the beginning of the school year. Permission will last until a new request is made, the student leaves school or a parent/carer provides a written withdrawal of taking images of their child.
- 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.
- The school will also ensure that when images are published, full names or personal information is not published.
- Pupils are not permitted to take, use, share, publish or distribute images of others within the school but are educated on gaining an individual's permission before taking, using or distributing photographs of others outside school.
- The use of digital/video images plays an important part in learning activities.
- The school will comply with the GDPR regulations as guided by EA.

Parents are informed that images taken at school events such as Sports Day and concerts are for personal use only and images of other children and staff should not be posted on social media.

Teaching and Support Staff: Password Security

Password security is essential for staff, particularly as they are able to access and use student data.

- All staff are expected to have secure passwords which are not shared with anyone.

- All staff are aware of their individual responsibility to protect the security and confidentiality of the school network, including ensuring that passwords are not shared and are changed periodically.
- Individual staff users must also make sure that workstations/iPads are not left unattended and are locked.

Students: Password Security

- All users and their parents read, discuss and digitally acknowledge that the Acceptable Use of the Internet and Digital Technologies Policy has been agreed.
- Students are expected to keep their passwords secret and not to share with others, particularly their friends. They are taught about appropriate use of passwords at an appropriate age, ability and aptitude.
- Pupils cannot access on-line materials or files on the school network, of their peers, teachers or others. Pupils may only access their own files on My School.

Cyber-Bullying

Cyber-bullying can take many different forms and guises including:

- **Email** – nasty or abusive emails which may include viruses or inappropriate content;
- **Instant Messaging (IM) and Chat Rooms** – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity;
- **Social Networking Sites** – typically includes the posting or publication of nasty or upsetting comments on another user’s profile;
- **Online Gaming** – abuse or harassment of someone using online multi-player gaming sites;
- **Mobile Phones** – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people; and
- **Abusing Personal Information** – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person’s permission.

Incidents of cyber-bullying will be dealt with in accordance with the School Anti-Bullying Policy, Discipline Policy and Pastoral Care Policy.

The Data Protection Act

All staff are regularly reminded of their responsibilities in relation to the Data Protection Act. In particular, staff must ensure that they, at all times, take care to ensure the safe keeping of personal data, minimising the risk of loss or misuse.

Staff are not permitted to remove personal data about a child from the school. Any data stored on the school system, and protected with a secure password, must be deleted from the device once it has been transferred to a secure location or once it is no longer of any

use. No personal data about a child should be stored on a removable device as there is always a risk of it being stolen or getting lost.

Technical Framework

Filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. The responsibility for the management of the school's filtering policy is held by Miss Loughrey. The school's filtering policy is to keep all computers under the default filtering system as administered by C2K.

Staff and pupils have a responsibility:

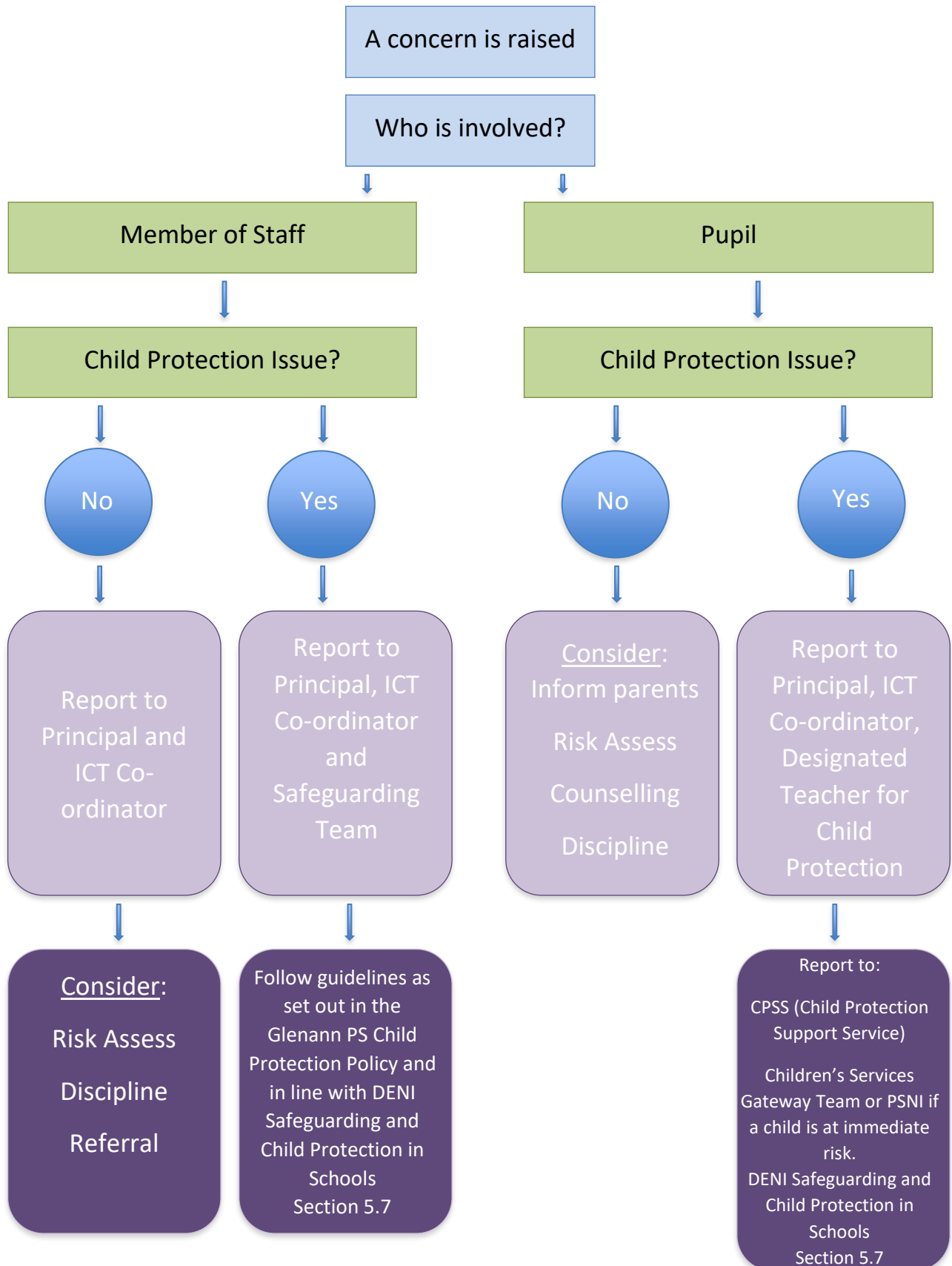
- to report immediately to the ICT Co-ordinators any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered; and
- users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials.

Managing Incidents / 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, involving children or staff.

- 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 Positive Behaviour Policy.

Handling an E-Safety Complaint



If you are in any doubt, consult the Principal, Designated Teacher for Child Protection (Mrs Bailey), Deputy Designated Teacher for Child Protection (Miss Loughrey) or the CPSS.

Sanctions

We believe it is important that the school has a culture under which users understand and accept the need for E-Safety regulations and adopt positive behaviours, rather than one in which attitudes are determined solely by sanctions. Incidents of technology misuse which arise will be dealt with in accordance with the school's Positive Behaviour Policy.

Minor school related incidents will be dealt with by the principal. This may result in parents being informed and a temporary ban on Internet use. Incidents involving Child Protection issues will be dealt with in accordance with the school's Safeguarding and Child Protection Policy. This will include involvement from the school Safeguarding Team or outside agencies in terms of advice and support. Further to this, should technology or online platforms be used as a means by which to bully another, the sanctions detailed in the Anti-Bullying Policy will be implemented.

Users will understand their responsibilities to report E-safety incidents. They will know and understand that there are clear systems for reporting abuse and understand that the processes must be followed rigorously. Incident reports will be logged by the principal and ICT Co-ordinator for future auditing, monitoring, analysis and for identifying serious issues or patterns of incidents. This will allow the school to review and update the E-Safety policy and practices.

Pupils are aware that any misuse of technology should be reported to a member of staff immediately. The Safeguarding Team understand how to report issues online, should the need arise, including to CEOP.

Approval of E-Safety Policy

Approved by Board of Governors

Acting Chairperson: *Mr F Close*

Date: 23 / 09 / 25

Acting Principals: *Mrs Bailey and Miss Loughrey*

Date: 23 / 09 / 25

Review Date: September 2026