COLERAINE GRAMMAR SCHOOL
ONLINE SAFETY POLICY

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within school and in their lives outside school. ICT can help everyone to learn. Children and young people have an entitlement to safe access when using the internet. The requirement to ensure that children and young people are able to use the internet and related communication technologies safely and appropriately is addressed as part of the wider duty of care to which all who work in schools are bound.

These technologies however, can put young people at risk by accessing illegal, harmful or inappropriate images, grooming, the distribution of images or personal details without their consent or knowledge and copyright infringement.

It is impossible to eliminate all risk completely. It is therefore essential, through good educational provision, to build pupils' resilience so they have the confidence and skills to face and deal appropriately with the risks to which they may be exposed. This policy will be used in conjunction with other school policies.

Schedule for Development, Monitoring and Reviewing Policy

Approval by the Board of Governors	March 2026
Implementation	The online safety coordinators are: VPs (Curriculum/Pastoral), Curriculum Leader (ICT)
Monitoring and review	Annually
The Board of Governors will receive an annual report on online safety (including anonymous details of online safety incidents)	This will be in conjunction with the Child Protection Report given to the Board of Governors each year.
Should serious online safety incidents take place, the following external persons or agencies should be informed	CPSSS EA (NE region) PSNI Chair of BoG

The school will monitor the impact of the policy using:

- Logs of reported incidents;
- Consultation with staff, pupils and parents.

Scope of the Policy

This policy applies to all members of the school community who have access to and are users of the school ICT systems both in and out of school. In relation to incidents that occur during school hours, the school will work cooperatively with the parents, staff and pupils to ensure the online safety of all involved, apply sanctions as appropriate and work to prevent such behaviour reoccurring.

In relation to incidents that occur outside of school hours, the school will work cooperatively with the pupils and parents to keep all pupils safe and prevent such behaviour reoccurring. Postings made outside school hours are primarily the responsibility of the parents. If inappropriate postings occur outside school hours which are intended to have a negative effect on any member of the school community, and these come to our attention, then the school will liaise with parents as to an appropriate way forward. We do, however, reserve the right to discipline a pupil for actions taken off-campus. Any further incidents which arise inside school as a result of earlier postings will be dealt with in accordance with School Policies.

All pupils and staff should be aware that by logging on to the C2K system they are agreeing to the C2K Acceptable Use Policy. The Acceptable Use Policy (AUP) is printed in pupil planners and must be signed at the start of the school year. The AUP is printed in staff planners and a hard copy must be signed by all staff at the start of the school year.

Roles and Responsibilities

Governors

The Board of Governors are responsible for the ratification of the Online Safety Policy and for reviewing its effectiveness. There is an appointed online safety Governor (Mrs H Hamilton) who will:

- meet with the online safety coordinators;
- monitor online safety incidents;
- report to the Board of Governors regarding online safety in school.

Headmaster and SMT

The Headmaster is responsible for ensuring the online safety of all members of the school community, though the day to day responsibility for this is delegated to the online safety coordinators. The Headmaster and SMT will follow school policy and procedures in the case of a serious online safety allegation being made against a member of staff.

The SMT:

- are responsible for providing appropriate CPD for online safety coordinators and other relevant staff to enable them to carry out their roles and train other colleagues, as relevant;
- will receive regular monitoring reports from the online safety coordinators.

Online safety coordinators

This role is shared between the CL (ICT) and the Vice Principals.

The coordinators:

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school Online Safety policy;
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place;
- provide training and advice for staff;
- liaise with C2K and the school ICT technical staff;

- receive reports of online safety incidents and create a log of incidents to inform future online safety developments;
- when required, meet with the online safety Governor to discuss current issues and review incident logs.

C2K Managers

The school will monitor that C2K online safety measures, as recommended by DENI, are working efficiently within the school.

The C2K Managers are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack in line with C2K;
- that the school, through C2K, meets required Online safety technical and password requirements;
- the filtering policy is applied and updated by C2K.

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety policy and practices;
- they have read, understood and signed the Staff Acceptable Use Policy;
- they report any suspected misuse or problem to the Online safety coordinators for investigation;
- All downloaded material in school on school systems has an educational content;
- all digital communications are on a professional level and only carried out using official school systems;
- Online safety issues are embedded in the curriculum and other activities;
- pupils understand and follow the Online Safety and Acceptable Use policies;
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities 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.
- they not use AI tools in ways that compromise data protection (governed by *UK GDPR and the Data Protection Act 2018*), confidentiality, or assessment integrity.

Safeguarding Designated Person

The designated person should be trained in Online safety issues and be aware of the potential for serious child protection or safeguarding issues which arise from:

- sharing of personal data;
- access to illegal or inappropriate materials;
- inappropriate on-line contact with adults or strangers;
- potential or actual incidents of grooming;
- cyber-bullying.

Pupils:

- are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy;
- should develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- must not use AI tools in ways that compromise academic integrity, data protection, or safeguarding (in conjunction with 'Coleraine Grammar School Examinations Malpractice Policy').

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking and use of images and on cyber-bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety policy covers their actions out of school, if related to their membership of the school.

Parents and Carers
The school will take every opportunity to help parents understand these issues through parents' evenings, the CGS website, literature and information about national and local online safety campaigns.

Education

Online safety is a focus in all areas of the curriculum:
- A planned online safety curriculum is a part of ICT/LLW and is regularly reviewed;
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Pupils are helped to understand the need for the Pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff temporarily remove those sites from the filtered list for the period of study.

Education – Parents and Carers
The school provides information for parents and carers through:
- School Website;
- Parents evenings - PSNI Chat Share Think programme.

Training – Staff
All staff receive online safety training as required and understand their responsibilities, as outlined in this policy.

Training – Board of Governors
Governors can, if available, take part in online safety awareness sessions.

Technical – infrastructure, equipment, filtering and monitoring
The school, through C2K, will be responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their Online safety responsibilities.

The Bring Your Own (BYOD) Policy has been implemented and pupils in Sixth Form may use devices brought in from home once the BYOD User Agreement has been returned to the school. A signature from a parent/carer is required.

Use of digital and video images
Staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:
- 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, for example, on social networking sites;

- Parents are welcome to take videos and digital images of their own children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital / video images;
- 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. Those images should only be taken in line with the guidance provided in the Acceptable Use Policy for Staff;
- Pupils must not take, use, share, publish or distribute images of others without their permission.

Dealing with incidents

Incidents will be dealt with by the online safety and Child Protection coordinators in line with legislation and the CGS Positive Behaviour Policy.

Data Protection

Personal data will be processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Communications

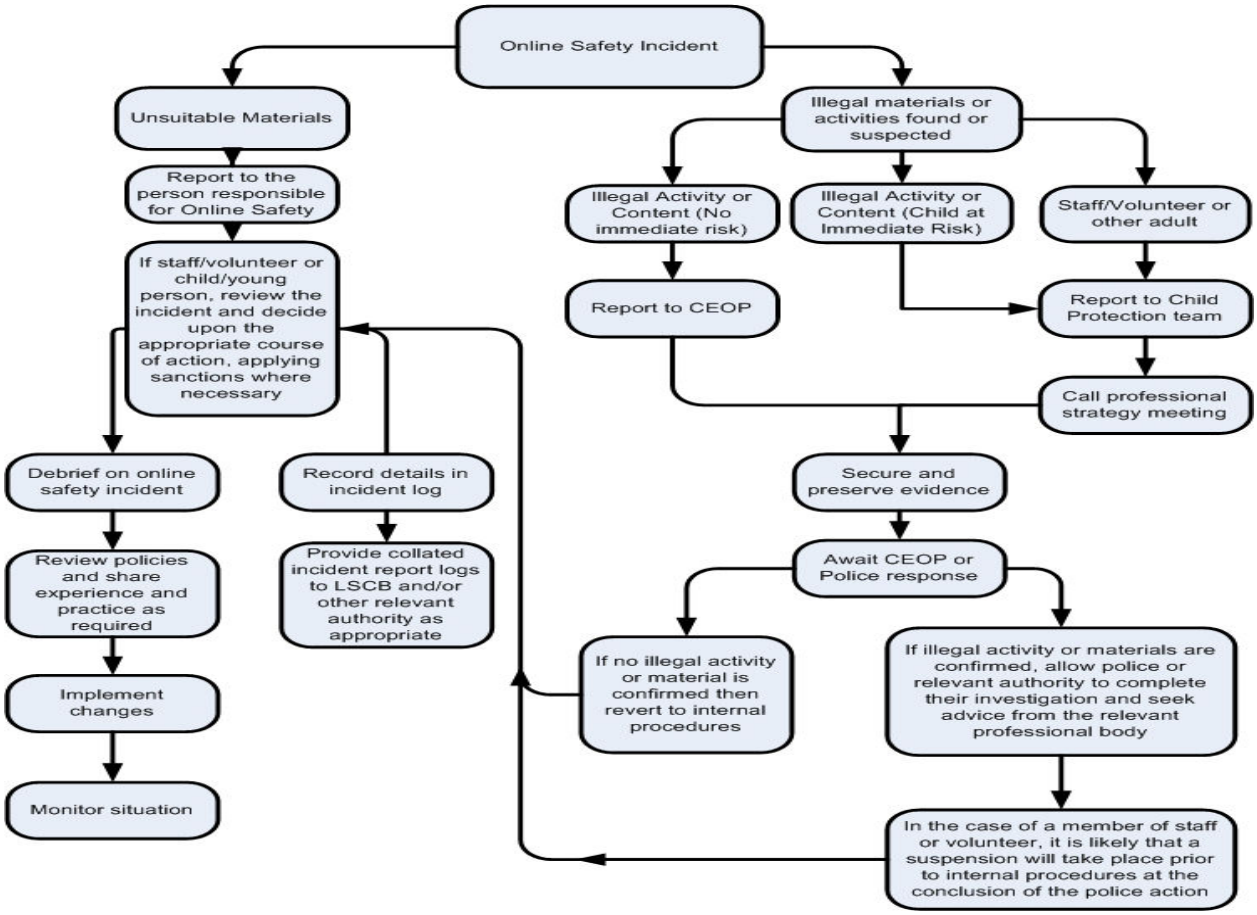
Our policy on the use of mobile phones and other digital devices is set out in a separate policy.

Unsuitable and inappropriate activities

In line with Staff Acceptable Use Policy, internet activity relating to for example child abuse images or distributing racist material is illegal and consequently banned from school systems. Staff must be professional in their use of the school system and not access or permit pupils to access any inappropriate material.

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 flowchart below 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:

- All online safety coordinators should be involved in the process of investigating an incident. This is vital to protect individuals if accusations are subsequently reported;
- The procedure will be conducted 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. The same computer will be used 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 EA (NE region) CPSSS;
- 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. Record all actions carefully.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. 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. Incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. Suspected or actual illegal or criminal activity will be dealt with through the Promoting Positive Behaviour Policy as a Level 3 incident with the potential consequence of suspension or expulsion.