New Machar School

E-Safety Policy

This e-safety policy was agreed	*October 2020*
The implementation of this e-safety policy will be monitored by the:	*E-Safety Coordinator and Senior Leadership Team*
Monitoring will take place at regular intervals:	*Once a year*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Kathryn Duncan, Laura MacFadyen, Brian Carle – Police/ other agencies if relevant*

This policy applies to all members of the school community (including staff, children, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school.

Responsibilities

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- staff are aware of the Acceptable Use of Technology in School
- they report any suspected misuse or problem to the *E-Safety Coordinator or Senior Leadership Team* for investigation and action;
- all digital communications with children/young people / parents / carers should be on a **professional level** *and only carried out using official school systems;*
- e-safety issues are embedded in all aspects of the curriculum and other activities;
- teachers 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 children/young people 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.*

Children / young people:

- are responsible for using the school digital technology systems in accordance with the Acceptable Use Policy for children/young people;
- have a good understanding 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. They need to understand the need to protect themselves and respect others when participating in social networks;
- 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 / use of images and on cyber-bullying;

- 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;
- should demonstrate an understanding of digital citizenship and how it links to their roles and responsibilities within the school.

Parents / Carers

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 work closely in partnership with parents on these issues through *parents' evenings, newsletters, letters, website / Glow and information about national / local e-safety campaigns / literature.* 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;
- access to parents' sections of the website / Glow and on-line pupil learning where relevant;
- their children's personal devices in the school (where this is relevant).

Policy Statements

Education – children

Whilst regulation and technical solutions are very important, their use must be balanced by educating children to take a responsible approach. The education of children in e-safety is therefore an essential part of the school's e-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- a planned e-safety curriculum should be provided as part of Computing / Health and Wellbeing / other lessons and should be regularly revisited. It may be delivered as an interdisciplinary learning unit;
- key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities. The emphasis in such messages should be on children and young people learning to protect themselves and respect others. As appropriate the planned programme should help children understand what Digital Citizenship means and how it relates to the roles and responsibilities outlined in the school's positive behaviour policy;
- children should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- children should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school;
- staff should act as good role models in their use of digital technologies the internet and mobile devices;
- where children / young people are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit;

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some parents may have extensive knowledge and expertise in this area and be able to support the school.

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

- *curriculum activities;*
- *letters, newsletters, web site, Glow;*
- *parents / carers evenings / sessions;*

- *high profile events / campaigns for example Safer Internet Day;*
- *reference to the relevant web sites / publications for example www.swgfl.org.uk* www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

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:

- a planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety personal learning needs of all staff will be carried out regularly
- 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;
- *the E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations;*
- *this E-Safety policy and its updates will be presented to and discussed by staff in staff / departmental meetings / INSET days;*
- *the E-Safety Coordinator will provide advice / guidance / training to individuals as required.*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children / young people instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and children / young people need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Young people should also be aware of potential risks of sharing personal / intimate photographs with friends as they may easily then be spread beyond their intended recipient. 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 children / young people 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, or sending inappropriate /intimate digital images which then may be shared further;**
- Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (such activity for personal use is exempt under 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 / carers comment on any activities involving other *children / young people* 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 on school equipment, the personal equipment of staff should not be used for such purpose;
- care should be taken when taking digital / video images that children / young people are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- children / young people must not take, use, share, publish or distribute images of others without their permission;
- photographs published on the website, or elsewhere that include children / young people will be selected carefully and will comply with good practice guidance on the use of such images;
- children/Young People's full names will not be used anywhere on a website or blog, particularly in association with photographs;
- written permission from parents or carers will be obtained before photographs of children / young people are published on the school website
- learners' work can only be published with the permission of the children / young people and parents or carers.

Data Protection

See Aberdeenshire Council Guidelines

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Children			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones or other camera devices		✓						✓
Use of other mobile devices for example tablets, gaming devices		✓						✓
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails				✓				✓
Use of messaging apps on school equipment				✓				✓
Use of social media on school equipment				✓				✓
Use of blogs (unrelated to school)				✓				✓

When using communication technologies the school considers the following as good practice:

- **the official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.**
- **users must immediately report, to the nominated person – in accordance with the school policy, 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;**
- **any digital communication between staff and children / young people or parents / carers (email, Glow etc) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications;*
-
- *children / young people should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;*

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyber-bully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school *or* local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

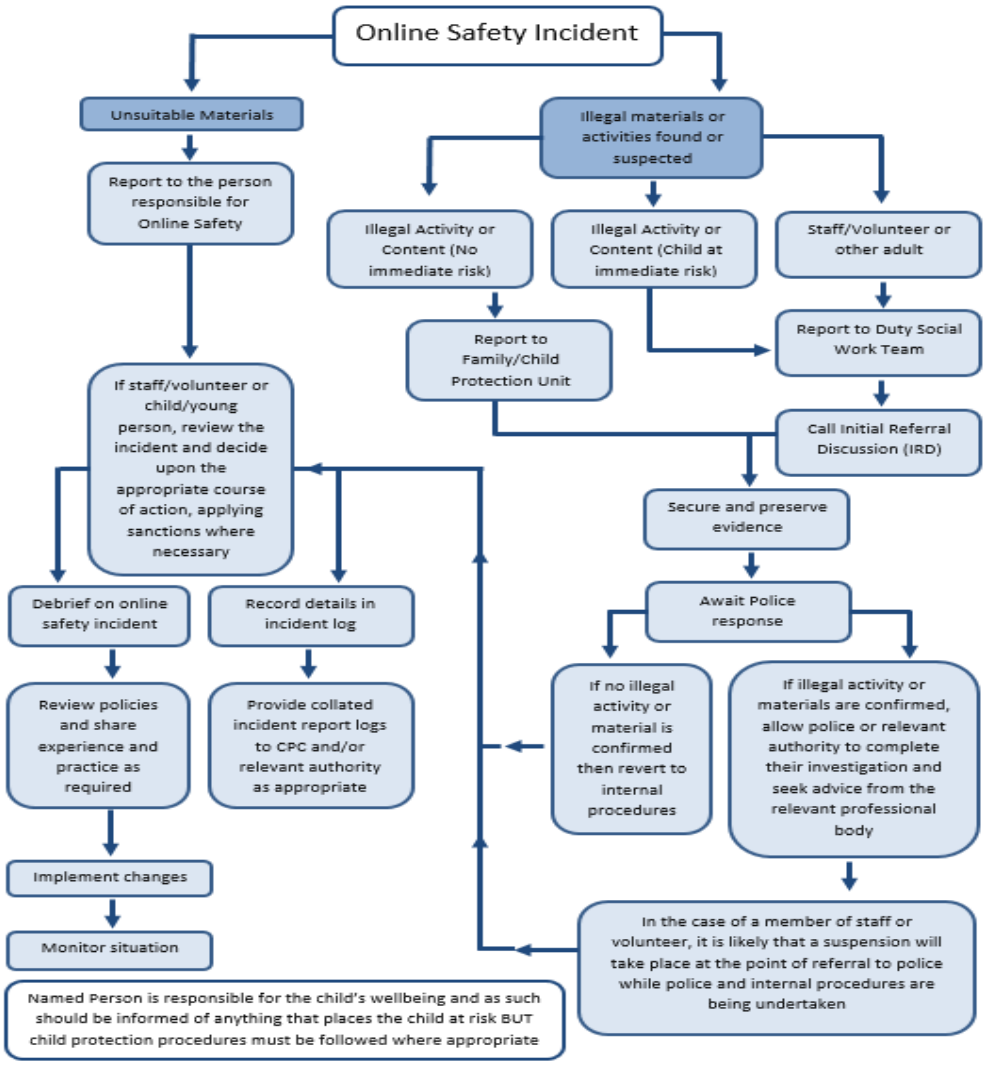
- training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues;
- clear reporting guidance, including responsibilities, procedures and sanctions;
- risk assessment, including legal risk.

School staff should ensure that:

- no reference should be made in social media to children / young people, parents / carers 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 the school or local authority;
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

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.


Online Safety Incident
Unsuitable Materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review policies and share experience and practice as required
Provide collated incident report logs to CPC and/or relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk BUT child protection procedures must be followed where appropriate
Illegal materials or activities found or suspected
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at immediate risk)
Staff/Volunteer or other adult
Report to Family/Child Protection Unit
Report to Duty Social Work Team
Call Initial Referral Discussion (IRD)
Secure and preserve evidence
Await Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police while police and internal procedures are being undertaken