

**E-Safety & Technologies Policy**

**Schedule for Development / Monitoring / Review**

The implementation of this e-safety policy will be monitored by the:**E-Safety Group** comprising of

     Headteacher

     Digital Technologies Coordinator

     Parents and Carers

     Digital Leaders from each class

The E-Safety Policy will be reviewed annually from date of approval (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.)

Should serious e-safety incidents take place, the following persons / external agencies should be informed:

     Headteacher

     Child Protection Officer

     Corporate IT

     Police

The school will monitor the impact of the policy using:

*• Logs of reported incidents*

*• 360 Online E-Safety Review Tool*

*• Surveys / questionnaires of*

**     *Staff*

**     *Focus groups of children*

**     *Parents/Carers*

**Scope of the Policy**

This policy applies to all members of the school community (including staff, pupils, parents / carers and visitors) who have access to and are users of school Digital Technology systems.

Hazlehead School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of any incidents of inappropriate e-safety behaviour that take place in school.

**Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

**Headteacher:**

• The *Headteacher* 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 *E-Safety Co-ordinator.*

• The Headteacher and another member of the Senior Management 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. (see flow chart on dealing with e-safety incidents – included in a later section – “Responding to incidents of misuse” and relevant Local Authority HR / other relevant body disciplinary procedures).

• The Headteacher is responsible for ensuring that the E-Safety Coordinator 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 Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

**E-Safety Coordinator:**

• leads the e-safety committee

• takes day to day responsibility for e-safety issues and has 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 Local Authority

• liaises with Corporate IT

• receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

• report regularly to Management Team

**Digital Technology Co- ordinator:**

* the Co-ordinator takes responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/ documents
* ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety event taking place
* keeps up to date with the needs of staff and school providing training and advice where necessary
* liaises with the local authority and associated school groups
* liaises with corporate IT
* keeps reports and a log of e-safety or Digital Technology incidents to inform future learning

**ICT Technical Staff:**

The ICT Technical Staff is responsible for ensuring:

**•**the school’s technical infrastructure is secure and is not open to misuse or malicious attack

• users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

• the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Coordinator for investigation / action / sanction

**Teaching and Support 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

• they have read, understood and signed the Staff Acceptable Use Policy

• they report any suspected misuse or problem to the Headteacher / E-Safety Coordinator for investigation / action / sanction

• all digital communications with students / pupils / 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

• Pupils understand and follow the e-safety and acceptable use policies

• they monitor the use of digital technologies, I-Pads, 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 students / 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

**Child Protection Officer**

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

• cyber-bullying

**Digital Technology Group:**

 The Digital Technology Group has responsibility for issues regarding Dig Tech and E- safety and the monitoring the e-safety policy including the impact of initiatives.

 Members of the group will assist the SMT and Digital Technology Coordinator with:

* the production / review / monitoring of the school e-safety policy / documents.
* mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
* monitoring network / internet / incident logs
* consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
* monitoring improvement actions identified through use of the 360-degree safe self-review tool
* updating and implementing of new strategies involving Digital Technologies across the school
* support the staff in the use of Digital Technology throughout the curriculum

**Students / Pupils:**

**•**are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use 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 I-Pads 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

**Parents / Carers**

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices/ tablets in an appropriate way. The *school* will take every opportunity to help parents understand these issues through *parents’ evenings, newsletters, letters and information evenings.* 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 such as mobiles, tablets, laptops etc which allow access to internet/webcams

**Policy Statements**

**Education – students / pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach.  The education of pupils in e-safety is therefore an essential part of the school’s e-safety provision. Children and young people 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 the Digital Technology/ Health and Wellbeing curriculum (eg Circle Time)  and should be regularly revisited

• Pupils 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.

• Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

• Pupils should be helped to understand the need for the student / pupil 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 tablet devices

• In lessons where internet use is pre-planned, it is best practice that 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.

• Where pupils are allowed to freely search the internet, pupils must be taught/shown how to use the filtered Google Safe Search while browsing and all staff should be extra 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.

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

• Curriculum activities

• Letters, newsletters, class online blogs

• Parents / Carers evenings / information sessions

**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 (incl. GDPR) training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training 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 (eg from 360 Safe) 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 / team meetings / INSET days.

• The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

**Technical – infrastructure / equipment, filtering and monitoring**

Aberdeen City Council Corporate IT work alongside schools in Aberdeen.  In these schools they are responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

**Use of 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 / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. 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 eg 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. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images – No pupil names will be published next to pictures.

• Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website

**Data Protection**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (GDPR) and in line with Aberdeen City Councils Data Protection Policy which states that personal data must be:

* Fairly and lawfully processed
* Processed for limited purposes
* Adequate, relevant and not excessive
* Accurate
* Kept no longer than is necessary
* Processed in accordance with the data subject’s rights
* Secure
* Only transferred to others with adequate protection.

Cont.

The school must ensure that:

It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

Responsible persons are appointed / identified

It has clear and understood arrangements for the security, storage and transfer of personal data

Data subjects have rights of access and there are clear procedures for this to be obtained

There are clear and understood policies and routines for the deletion and disposal of data

There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

• Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

**•**the data must be encrypted and password protected

**•**the device must offer approved virus and malware checking software

**•**the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

 **Responding to incidents of misuse**

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.

**Illegal Incidents**

If there is any suspicion that the web site(s) concerned may contain suspected illegal activity, refer to the right-hand side of the Flowchart 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 / volunteer 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 schooland 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 of reviewing devices / internet sites (responding to incidents of misuse)**

|  |  |
| --- | --- |
| Group |   |
| Date |   |
| Reason for investigation |   |

**Details of first reviewing person**

|  |  |
| --- | --- |
| Name |   |
| Position |   |
| Signature |   |

**Details of second reviewing person**

|  |  |
| --- | --- |
| Name |   |
| Position |   |
| Signature |   |

**Name and location of computer used for review (for web sites)**

|  |
| --- |
|   |

**Web site(s) address / device + reason for concern**

|  |  |
| --- | --- |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

**Conclusion and Action proposed or taken**

|  |  |
| --- | --- |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

**Template Reporting Log**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Reporting Log | Signature |  |  |  |  |  |  |  |  |
| Incident Reported by |  |  |  |  |  |  |  |  |
| Action taken | By whom? |  |  |  |  |  |  |  |  |
| What? |  |  |  |  |  |  |  |  |
| Incident |  |  |  |  |  |  |  |  |
| Time |  |  |  |  |  |  |  |  |
| Date |  |  |  |  |  |  |  |  |