Dunottar School

E-Safety Policy

Contents Page

E-Safety Policy

Policy Statement

The e-safety policy is a key element of the IT Policy as it is about the safe and responsible and ethical use of online technologies. It covers accessing online resources through computers, tablets, ipads, smart phones and any other internet enabled device safely and effectively. In conjunction with the Social Media Policy, it includes new social media tools and other emerging trends. It should cover a range of issues and not condemn the use of tools but rather address how to use them safely. This should include how to comment appropriately in many different forums, including social media and not being just a bystander. An essential part of this is how to report concerns, online and offline.

This policy applies to all members of Dunottar School who have access to and are users of school ICT systems, both in and out of the school.

Dunottar School is fully committed to ensuring the application of the E-Safety Policy and other related technology policies are non-discriminatory in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunity Policy document.

Dunottar School seeks to implement this Policy through adherence to the procedures set out in the rest of this document.

In line with our Provision of Information Policy, this document is available to all interested parties on our website and hard copies are available, on request, from the school main office.

This e-safety policy should be read in conjunction with other policies with the over-arching Technologies Policy but with particular reference to the IT Policy, Mobile Devices Policy, Social Media Policy and Internet Filtering Policy .

The next date for review is October 2019 or when events or legislation require.

Key Personnel

- Mr T Stevens (Network Manager)
- Mr Marc Broughton- E-Safety Co-ordinator (Deputy Head, Pastoral)
- Mr Gary Richards- E-Safety Governor (LGB)

Key personnel providing external e-safety training

- Mr James Garnett (Deputy Director of Technology, United Learning)

Area of risk:

Communicating with children electronically

Using online services and sites, not provided by Dunottar School, to communicate between a teacher and a student may put one or both participants at risk. This is because; it is not open and transparent. In addition, there is no audit trail, as Dunottar School does not control the communication channel so cannot access the data, and so it is impossible to monitor.

E-Safety in the Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. E-safety 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 / PHSE / other lessons and should be regularly revisited
- Key e-safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students will 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 when using technology.
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students understand and sign the Student Acceptable Use Agreement and are encouraged to adopt safe and responsible use both within and outside school
- Staff will act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that students 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.
- Staff should be mindful that they must differentiate between different Year groups when planning lessons using the internet.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the students visit. Additional monitoring of individual internet use is also in place via Securus.
- When using apps or websites, Dunottar School will assess their compliance for GDPR and if necessary complete a DPIA.

E- Safety and Staff

All staff must read and sign the ICT Acceptable Use Policy for Staff, before using any school ICT resource. The school will maintain a current record of all staff who are granted access to school ICT systems. Any person not directly employed by the school will be asked to sign the ICT Acceptable Use Policy for Staff before being allowed to access the internet from the school site.

All staff will be directed to the School's E-Safety Policy, and related policies and procedures, and their importance explained. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

E- Safety and Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Dunottar School provides children and young people help and support so they can recognise and avoid and manage e-safety risks, build their resilience and use technology responsibly.

All students must read and sign the ICT Acceptable Use Policy for Students, before using any school ICT resource. The school will maintain a current record of all students who are granted access to school ICT systems.

The School controls access to social networking sites, and considers how to educate students in their safe use, such as the use of passwords. This control may not mean simply blocking every site, which is usually counter-productive; it is often more effective and valuable to monitor and educate students in their use. Newsgroups will be blocked unless a specific use is approved.

Students are advised never to give out personal details of any kind which may identify them or their location. Students must not place personal photos on any social network space provided in any school learning platform or application. In addition, students and parents are advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for primary and secondary aged students.

Students are advised to use nicknames and avatars when using social networking sites and to consult adults at once if someone they have encountered online requests to meet them.

E- Safety and 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 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:

- Letters
- Parent evenings
- High profile events, campaigns and visiting speakers e.g. Dunottar's 'Virtually safe' Safer Internet Week
- Reference to the relevant web sites / publications e.g. CEOP (www.ceop.police.uk) and Child line (www.childline.org.uk) which can also be found via the school website

Parents are encouraged to attend evenings and events in order to, protect their children's safety, better inform themselves of the services that their children may access and the related benefits and risks.

E-safety Information

Internal resources

E-safety information can be accessed by students and teachers via the school website and on the United Hub.

External resources

External sources of reliable information on the safe use of the internet, training resources, parental information sites, can be accessed on the useful links page of the school website.

Reporting Procedures

Staff must use the helpdesk system to alert members of the IT department and inform the E-Safety Co-ordinator. Students should report, any instances of occasions where unsuitable or inappropriate material is accidentally viewed by the student, directly to their teacher who will then report it on to the E-safety co-ordinator.

Monitoring Success

In order to monitor the success of e-safety in the school Dunottar school:

- Gets weekly search query reports which show what is being looked at on the internet

Name of owner/author	M.Broughton/ M.Thomas	
Authorised By	M.Broughton	Oct 2016
Date Document Reviewed	MB/ST	Oct 2016
Date Document Reviewed	MB/ST	Oct 2017
Date document updated	ST	Jan 2018- Change of Network Manager
Date document updated	ST	April 2018- Change of Network Manager
Update	ST/AD	Jul2018
Review	ST/MB	Oct 2018
Review	ST/MB	*Oct 2018*
Next Review date	Oct 2019	*Oct 2019 or when events or legislation require*
Governor responsible for Policy	Gary Richards	