E-Safety

Date: September 2016

Review Date: September 2017

Policy Statement
For clarity, the E-Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents / carers.

Safeguarding is a serious matter; at Durand Academy we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

This policy is available for anybody to read on the Durand Academy website; upon review all members of staff will sign as read and understood both the E-Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Pupils Acceptable Use Policy will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body
The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

Head Teacher
Reporting to the governing body, the Head Teacher has overall responsibility for E-Safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer (or more than one), as indicated below.

The Head Teacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated E-Safety Officer(s) has had appropriate CPD in order to undertake the day to day duties.
- All E-Safety incidents are dealt with promptly and appropriately.

E-Safety Officer

The day-to-day duty of E-Safety Officer is devolved to Jerome Hall

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head Teacher, governing body on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the E-Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical E-Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical E-Safety measures, i.e. internet filtering reporting function; liaise with the Head Teacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any E-Safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety officer and Head Teacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.
- The IT System Administrator password is to be changed on a monthly (30 day) basis.

All Staff
Staff are to ensure that:

- All details within this policy are understood. If anything is not understood, it should be brought to the attention of the Head Teacher.
- Any E-Safety incident is reported to the E-Safety Officer (and an E-Safety Incident report is made), or in his/her absence to the Head Teacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Head Teacher to make a decision.
- The reporting flowcharts contained within this E-Safety policy are fully understood.

All Pupils
The boundaries of use of ICT equipment and services in this school are given in the pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers
Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings and school newsletters the school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the pupil Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology
Durand Academy uses a range of devices including PC's, laptops, Apple Macs. In order to safeguard the pupil and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Watch Guard software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.

Email Filtering – we use Sophos software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or

script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change on a termly basis or if there has been a compromise, whichever is sooner. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this E-Safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Social Networking – there are many social networking services available; Durand Academy is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Durand Academy and have been appropriately risk assessed; should staff wish to use other social media; permission must first be sought via the E-Safety Officer who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and pupils in school.

In addition, the following is to be strictly adhered to:

- There is to be no identification of pupils using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".

- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools' attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any E-Safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Head Teacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Durand Academy will have an annual programme of training which is suitable to the audience.

E-Safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD.

Cyber-Bullying

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/ herself.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hikacking/ cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, to include Facebook and Youtube

At Durand Academy we educate our students in the proper use of telecommunications and about the serious consequences of cyber-bullying.

Sexting
Sexting is images or videos generated

- By children under the age of 18, or
- Of children under the age of 18 that are of a sexual nature or are indecent

these images are shared between young people and/or adults via a mobile phone, handheld device, computer, 'tablet' or website with people they may not even know

Sexting disclosures should follow the normal safeguarding practices and protocols (see Cp & Safeguarding policy)

Please see our Anti-Bullying Policy

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an E-Safety incident, reported to the E-Safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the E-Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or pupil, or IT support.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head

Teacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the E-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the safety officer as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

E-Safety – like health and safety, E-Safety is the responsibility of everyone to everyone. As such you will promote positive E-Safety messages in all use of ICT whether you are with other members of staff or with pupils.

E-Safety Officer – Mr. J. Hall