



*Placing children's rights at the heart of all
we undertake.*

respect integrity humility equality care
towards all

Dosthill Primary Academy

On Line Safety Policy

Reviewed by: Rebecca Nicholson

Date: June 2019

Approved by: Governing Body

Date: 25th June 2019

Next review due: September 2019

Aims and Values

Our core moral purpose is encapsulated in the vision statement for the school: Striving for excellence in an inspirational climate where learning is nurtured and secured. Our core values permeate our every breath at Dosthill Primary Academy where everyone is selflessly committed to:

- Promising Academic Achievement.
- Crafting Character Skills for Life.
- Ensuring Excellence for All.
- Inspiring Each other/Achieving Together.

Our aim is that everyone in our Dosthill Family grows in confidence to achieve their ambitions and dreams with courage and kindness. We promise to provide a caring ethos where all children have the confidence to explore, dream and discover so that every valuable second of the day is a learning adventure.

Rights Respecting School

Article 13

You have the right to find out things and share what you think with others, by talking, drawing, writing or in any other way unless it harms or offends other people.

Article 17

You have the right to get information that is important to your well being, from radio, newspaper, books, computers and other sources. Adults should make sure that the information you are getting is not harmful, and help you find and understand the information you need.

Rationale/principles

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning.

National guidance suggests that it is essential for schools to take a leading role in e-safety. Becta in its "Safeguarding Children in a Digital World" suggested:

"That schools support parents in understanding the issues and risks associated with children's use of digital technologies. Furthermore, Becta recommends that all schools have acceptable use policies, and ensure that parents are aware of the procedures for e-safety within the school. Recognising the growing trend for home-

school links and extended school activities, Becta recommends that schools take an active role in providing information and guidance for parents on promoting e-safety messages in home use of ICT, too."

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

"One of the strongest messages I have received during my Review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to Government in the following areas: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote learner achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with *all* other school policies (eg behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build learners resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Curriculum

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that learners 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 learners are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- Learners 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

The Public Sector Equality Duty (PSED)

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Roles and Responsibilities

Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

- The E-safety co-ordinator for the school is [Mrs C Keay, Headteacher](#).
- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community
- The Headteacher and another member of the [SLT](#) 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.

The ICT Technician, [R Byrne](#), is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- the school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that he keeps up to date with e-safety technical information in order to effectively carry out his e-safety role and to inform and update others as relevant

Teaching staff, support staff, Governors and volunteers 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 school Staff Acceptable Use Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation.
- digital communications with learners (email / LP365 / voice) should be on a professional level.
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- learners understand and follow the school e-safety and acceptable use policy
- learners have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned learners 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.

Learners:

- are responsible for using the school ICT systems in accordance with the Learner Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- 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
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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

Parent/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 therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / LP365 and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy

- accessing the school website / VLE / on-line student / pupil records in accordance with Dosthill's Acceptable Use Policy.

Internet Use and Access (see acceptable use agreements for Dosthill Primary School)

Education and Training

Learners

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of learners in e-safety is therefore an essential part of our 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 education will be provided in the following ways:

- A planned e-safety programme will be provided as part of ICT / PSHE / other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. One lesson once a term will be explicit E-Safety, and starters will revisit this regularly during other sessions.
- Key e-safety messages will be reinforced in assemblies which will be planned throughout the year.
- Learners 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
- Learners will be helped to understand the need for the learners AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- AUP for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

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

- Letters, newsletters, web site, LP365
- Open evenings
- Class productions

Staff – Education and Training

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:

- 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 Agreement
- This E-Safety policy and its updates will be presented to and discussed by staff
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required

Governors - Training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / e-safety / health and safety / child protection.

Publishing learner's images and work

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and learners instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying 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 learners 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.

Parents/Carers are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

- Staff 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.
- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission

- Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images.
- Learners 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 learners are published on the school website
- Learners work can only be published with the permission of the learners and parents or carers.

Social networking and personal publishing

Dosthill Primary Academy controls access to social networking sites, and educates learners in their safe use.

Newsgroups are blocked unless a specific use is approved.

Learners are advised never to give out personal details of any kind which may identify them, their friends or their location.

Learners and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged learners.

Learners are advised to use nicknames and avatars when using social networking sites.

Learning Platforms

The contact details for the school will be kept up to date and will include name, address, e-mail and telephone number.

The Head teacher will take overall editorial responsibility and ensure content is accurate and appropriate.

Filtering

The school will work with the LA, DcFS and the Internet Service Provider to ensure systems to protect learners are reviewed and improved. Systems in place are filtering and Impero.

If staff or learners come across unsuitable on-line materials, the site must be reported to the Headteacher.

Managing videoconferencing & webcam use

Videoconferencing should use the educational broadband network to ensure quality of service and security.

Learners ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the learner's age.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Technologies such as mobile phones and iPads with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. Learners will be educated through the methods set out in this policy.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden. [Pupil and visitors mobile phones must be handed in to the office and can be returned at the end of the visit/day.](#)

The use by learners of cameras in mobile phones will be kept under review.

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

Staff will be issued with a school phone where contact with learners is required or where mobile phones are used to capture photographs of learners.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.
 - 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.
-

Policy Decisions

All staff including visiting staff, must read and sign the 'Acceptable ICT Use Agreement' before using school ICT resources.

The school will keep a record of all staff and learners who are granted internet access. Learners will only sign another AUP when there is a change in the policy. These will be kept up to date if a member of staff leaves for example.

At Key Stage One, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

Assessing risks (see Acceptable Use Agreements)

Handling e-safety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the Headteacher.

Community use of the Internet

Dosthill Primary Acaemy will liaise with local organisations to establish a common approach to e-safety.

Introducing the e-safety policy to pupils

E-Safety rules are posted in all rooms on all computers via Impero. All learners will be asked to sign an user agreement which details the rules around their online usage.

Learners are informed that network and Internet use will be monitored and appropriately followed up.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school Web site and through Class teams from September 2019.

Dosthill Primary Academy will maintain a list of e-safety resources for parents/carers. (See Appendix 2 below)

Monitoring and Evaluation

This is carried out in a variety of different ways including:

- Staff highlighting relevant statements in the Building Blocks.
- Learning walks by SLT
- E-safety awareness including workshops with the parents/carers.
- Planning on Teams
- Impero checks of the system by RByrne and Becky Nicholson/
- Areas for development from learning walks, workshops, etc. are reviewed and built upon.
- Pupil conferencing/Book reviews
- Parent/Carer conferencing.
- Staff conferencing.

Dissemination

This policy was re-written in April 2013.

It is distributed to Parents/Carers via the school website.

Staff and governors have access to this policy via teams

A summary version of this policy is also available and sent out as a hard copy to Parents/Carers, staff and Governors every September.

Acknowledgements

Kent Schools Core e-Safety Policy and Audit 2008 Children, Families, Health and Education Directorate

<http://www.staffsscb.org.uk/e-SafetyToolkit/>

Internet Use and Access (see acceptable use policy for Dosthill Primary School)

Members of the SWGfL E-Safety Group and the SWGfL E-Safety Conference Planning Group

DCSF

Becta

NAACE

National Education Network (NEN)

London Grid for Learning

Kent County Council

Northern Grid for Learning

Byron Review – Children and New Technology – “Safer Children in a Digital World”