DURLSTON
PREP & SENIOR SCHOOL

6.4a Child Protection (Safeguarding) Policy
E-Safety Policy
including the Early Years Foundation Stage

Introduction

It is the duty of Durlston School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

There are four main areas of risk for online safety:

- CONTENT – being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, fake news, self-harm, anti-Semitism, radicalisation and extremism
- CONTACT – harmful online interaction with other users, e.g. peer to peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- CONDUCT – personal online behaviour that increases the likelihood of, or causes harm e.g. online bullying, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography)
- COMMERCE – risks such as online gambling, phishing, financial scams and inappropriate advertising.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites; Email and instant messaging; Blogs; Social networking sites;
- Chat rooms; Music / video downloads; Gaming sites;
- Text messaging and picture messaging; Podcasting; Online communities; and
- Mobile internet devices such as smart phones, smart watches and tablets.

This policy, supported by the Acceptable Use policy for all staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding (incl Staff Behaviour); Behaviour Management; Anti-Bullying;
- Data Protection and PSHE.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Durlston, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy for all staff and pupils, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, Chromebooks etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches etc.).

Roles and responsibilities

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The Governors are also responsible for doing all they can to limit children's exposure to risks from the school IT system. As part of this process, the governing body should ensure that that the school has appropriate filters and monitoring in place and regularly review their effectiveness

2. Headmaster and the Senior Leadership Team

The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for e-safety.

In particular, the role of the Headmaster and the Senior Management Team is to ensure that staff are aware of the school e-safety policy and the procedures that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. IT Manager

The school's IT staff member has a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They with the assistance of the Smoothwall monitoring team monitor on a daily basis the use of the internet and emails as well as maintaining content filters. Inappropriate usage is reported to the Headmaster, Head of Upper Prep/Senior School or Head of Middle Prep. A daily report of web filter breaches as well as live alerts is sent out to the Head and Head of Senior School.

4. Teaching and support staff

All staff are required to sign the Acceptable Use Policy (*see wording on pages 13-14) each year when accessing the school's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

5. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy (*see wording on pages 14-16), and for letting staff know if they see IT systems being misused.

6. Parents

Durlston believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. Parents are responsible for endorsing the school's Acceptable Use Policy.

Education and training

1. Staff: awareness and training

New staff receive information on Durlston's e-Safety and Acceptable Use policies as part of their induction.

All staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines. The signing of the Acceptable Use Agreement helps reinforce this message.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. With the introduction of Chromebooks and laptops in the Senior School, staff should be vigilant in all areas of the school in respect of this matter.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the Headmaster.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety (including recognising online sexual exploitation, stalking and grooming), the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Headmaster or any member of staff at the school. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities. This is largely done in the IT lessons, but it is also discussed in PSHE and other lessons, when appropriate.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-Bullying Policy). Pupils should approach their form teacher, their IT teacher as well as parents, peers and other school staff for advice or help if they experience bullying issues when using the internet and related technologies.

Online learning has been a factor in recent years; children using their school accounts are subject to the filtering and monitoring systems of the school when using these accounts in lockdown learning. Links to helpful sites were provided, and will continue to be provided, if lockdown learning reoccurs.

3. Parents

The school seeks to work closely with parents in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. By sharing the curriculum online, we will aim to let parents know of what children will be asked to do online and whether there is likely to be interaction with people online.

The school recognises that not all parents may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. This is organised to occur on an annual basis. More recently, with decreasing attendance at these events, we have switched to a service provided by Knowlsley. This provides monthly newsletters to parents, video training for staff, parents and governors as well as pupils.

Policy Statements

1. Use of internet and email

Staff

Staff must not access any website or personal email which is unconnected with school work or business whilst teaching / in front of pupils. Such access may only be made whilst in staff/non pupil areas of school.

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to Headmaster 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Facilities Manager.

Any online communications or use of social media must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Durlston into disrepute;
- breach confidentiality;
- breach copyright;

- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents must be professional in tone and content. Under no circumstances may staff contact a pupil or parent in relation to work by using their or any other personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

School staff must ensure that their use of email at work always complies with data protection legislation and confidential or personal data must not be sent electronically via email unless it is encrypted. Staff should be appropriately trained and should ensure they use appropriately secure email systems to share any sensitive or personal information.

Pupils

No pupils are allowed mobile phones on the school site unless express permission is given by the Headmaster. If they are to be used in IT lessons, they should be left in Reception before and after the lesson.

There is strong anti-virus and firewall protection on our network. Most spam emails and certain attachments will be blocked automatically by the email system.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to Headmaster or another member of staff.

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted

should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a sexual nature directly to the Headmaster or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored. Certain websites are automatically blocked by the school's filtering system

2. Vulnerable children

Vulnerable children are more likely to take risks in real life as well as online therefore there needs to be careful consideration around the support and education provided to these pupils, their teachers and carers.

3. Data storage and processing (including Cloud Storage)

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server or Domain controlled cloud storage (Durlston One Drive or Durlston Google Drive) only. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, and the Facilities Manager should be consulted about encryption should this be authorised. Passwords to Cloud accounts must be of a strength specified by the school, kept secure and under no circumstances shared with other individuals. If at any stage it is necessary and authorised to email data to a third party, e.g. future schools, this must be encrypted as per school policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Headmaster.

4. Filtering and Monitoring

No filtering or monitoring solution can offer schools and setting 100% protection from exposure to inappropriate or illegal content, so it is important to take other reasonable precautions to safeguard children and staff. Such methods may include appropriate supervision, requiring children and staff to sign an

Acceptable Use Policy (AUP), a robust and embedded online safety curriculum and appropriate and up-to-date staff training etc. A reliance on filtering and monitoring alone to safeguarding children online could lead to a feeling of complacency which may put children and adults at risk of significant harm.

If obscene searches are discovered via the monitoring system, then the child should be talked to and the parents contacted, via phone or email as well as the Pupil Record Book. Any punishment will depend on the age of the child and the search terms entered. Staff should check the sites viewed to establish why they have slipped through the filtering system. If that is the case, then this should be reported to the IT manager and the Headmaster. Please see Emergency Procedures later in the policy.

On a half-termly basis, at least, the monitoring and filtering histories should be investigated by the IT administrator and other staff as appropriate. Any sites that are inappropriate, but have been viewed, e.g. shopping sites, should be blocked by the IT administrator.

Governing bodies must be careful that "over blocking" does not lead to unreasonable restrictions as to what the children can be taught with regard to online teaching and safeguarding.

5. Password security

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers);
- not to write passwords down (as appropriate per age group); and
- not share passwords with other pupils or staff.
- Staff passwords should be changed on a regular basis.

6. Misuse

Durlston will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the HCSP. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying Policy.

7. Radicalisation

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils. The Smoothwall system prevents access to harmful material.

8. Cyberbullying

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone.

Cyberbullying may not always be intentional and repeated in the same way that traditional offline bullying is. Repeated harassment online could include an initial concern which is then shared or endorsed by others such as by “liking”, “sharing” or “commenting”. People may not feel that they are bullying by doing this and single issue may become more serious. It is very important that all incidents of online abuse are addressed as early as possible to prevent escalation.

Education staff, parents and young people have to be constantly vigilant and work together to prevent this and tackle it wherever it appears. Cyberbullying is a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community.

9. Consensual and non-consensual sharing of nude and semi-nude images and videos (a.k.a. Youth Produced Sexual Imagery or Sexting)

Please also see guidance produced by government on this issue:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
(last updated March 2024)

This can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. These images may be shared between children and young people and/or adults via a mobile phone, webcam, handheld device or website. Children and young people will always look to push the boundaries, especially when they go through puberty and are an age where they are more sexually and socially aware. Children typically do not use the term “sexting”, usually referring to the images as “selfies” and may decide to send such pictures or videos for many reasons. For younger children (early years and primary school aged) indecent images or videos may be taken or shared out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour or even exploitation due to blackmail from a friend, partner, or other on or offline contact. There can also be emotional and reputation damage that can come from having intimate photos forwarded to others or shared online including isolation, bullying, low self-esteem, loss of control, creating of a negative “digital footprint” or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation.

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence and from the age of 18, fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (this includes downloading or opening an image that has been sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with consent. “Sexts” may be viewed as police evidence and it is essential that schools secure devices and seek advice immediately when dealing with concerns.

‘Keeping Children Safe in Education’ 2024 highlights the need for all members of staff to be aware that abuse can be perpetrated by children themselves, including sexting, and there is a need for all members of staff to be aware of concerning behaviour and appropriate safeguarding responses.

It is essential that schools and settings handle consensual and non-consensual sharing of images as carefully as possible and offer support to all parties involved whilst abiding by the law and also do not compromise police investigations. Should an incident arise which necessitates criminal investigation then it may require the seizure of the phone/device and any other devices

involved or identified as potentially having access to the imagery. Schools and settings should ensure the existing policies regarding seizing and searching are robust and up-to-date.

Please follow link to resources provided by Safer Internet Centre:
https://saferinternet.org.uk/guide-and-resource/sexting-resources

10. Indecent Images

The law regarding indecent images of children - specifically (but not limited to):

- The Sexual Offences Act 2003 (England and Wales) defines a child, for the purposes of indecent images, as anyone under the age of 18. The Civic Government (Scotland) Act, 1982 replicates this.
- The Sexual Offences Act 2003 (England and Wales) provides a defence for handling potentially criminal images and this is supported by a Memorandum of Understanding which provides guidance on what is and is not acceptable.

It is an offence to possess, distribute, show and make indecent images of children. Making of and distributing indecent images of children includes printing and viewing them on the internet otherwise known as 'downloading'. More information about these offences can be found within the legal framework section.

Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of school computer equipment, schools should determine the level of response necessary for the offence disclosed. The decision to involve Police should be made as soon as possible if the offence is deemed to be out of the remit of the school to deal with. If schools are unsure if an issue is of a criminal nature then the Designated Safeguarding Lead should seek advice Where it is determined that an offence has been committed and that a police investigation is warranted, all measures to preserve evidence should be undertaken. If an officer decides that equipment needs to be seized, then they will need to determine if the equipment is networked. If in doubt as to whether the server should be seized or not, officers should seek advice from the Police Digital Forensic Unit, as seizure of the server will have a significant impact on the school. It is essential that schools are aware of this possibility and they should ensure that measures are in place to enable the school's computer network to continue functioning should this situation arise.

In cases where a suspect picture or photograph is discovered it should also be borne in mind that a person could be guilty of the offence to 'Make' and 'Distribute' if they print or forward the image.

11. Harmful Online challenges and online hoaxes

There is material available online that can help parents and carers in dealing with online challenges and hoaxes, and directs them to where they can get help and support.

https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes

Emergency Procedures

Failure of Filtering Service

Pupils should be trained to switch off images if an inappropriate image comes up on the screen. It should then become second nature to the children to switch off the screen as soon as they see anything unacceptable.

If it becomes apparent that inappropriate images are being seen, e.g. pornographic images, radicalisation etc then pupils should be taught and encouraged to click off the image and report the matter to a member of staff. The member of staff should inform the HM. The HM should instruct Internet access to be shut down until the reason for the breach in the system is discovered.

Parents of children affected should also be informed, as should both the Chair of Governors and the Safeguarding Governor.

When the breach has been isolated and repaired and the HM, together with the IT manager and appropriate Governors are confident in the security of the system, and that the filtering and monitoring system is working effectively, then the internet can be switched on again.

If the breach is discovered directly by the member of staff, then the same procedure should be followed. Please refer to appendix – Responding to Online Incident Involving Pupils.

Complaints

As with all issues of safety at Durlston if a member of staff, a pupil or a parent has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Headmaster in the first instance, who will liaise with Senior Management Team, and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using an Incident Report form and reported to the school's Headmaster, Richard May, in accordance with the school's Child Protection Policy.

Based on ISBA and Online Safety Policy and Guidance – Hampshire County Council

Approved by Board: Nov 2023

Last review: September 2024

Next Review: September 2025

Durlston Staff Acceptable Use Agreement

This covers the use of all digital technologies in school: i.e. **email, Internet, intranet, network resources,** learning platform, software, communication tools, **equipment and systems.** Staff sign up to this when they access the school system for the first time each year,

I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.

I will not reveal my password(s) to anyone.

I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.

I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school systems.

I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network and data security policy.

I will not engage in any online activity that may compromise my professional responsibilities.

I will only use the approved email system(s) for any school business.

I will not browse, download or send material that could be considered offensive to colleagues.

I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the *appropriate line manager / school named contact*.

I will not download any software or resources from the Internet that can compromise the network or might allow me to bypass the filtering and security system or are not adequately licensed.

I will check copyright and not publish or distribute any work including images, music and videos, that is protected by copyright without seeking the author's permission.

I will not connect any device (including USB flash drive), to the network that does not have up-to-date anti-virus software.

I will not use personal digital cameras or camera phones or digital devices (without permission) for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.

I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the *appropriate system or staff-only drive within school*.

I will follow the school's policy on use of mobile phones / devices at school.

I will use 3Sys in accordance with school protocols.

I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.

I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.

I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.

I understand that all Internet and network traffic / usage can be logged and this information can be made available *to the Head / Safeguarding Lead* on their request.

I understand that Internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.

I understand that failure to comply with this agreement could lead to disciplinary action.

Durlston Pupil Acceptable Use

These rules will keep everyone safe and help us to be fair to others.

- I will not do anything to hurt and upset other people.
- I will only use the school computers to view websites my teacher allows.
- I will not look at or change other people's files.
- I will keep my passwords secret.
- I will not give away personal information online.
- I will not bring in programs from home to use on the school campus.
- I will talk to my teacher or a member of staff if I see anything I am unhappy with or unsure about.
- I will not access any websites or play any games that I am not old enough to access.
- I will not visit chat rooms, social network sites, personal email or similar on the school computers.
- I am aware that the school is monitoring all my activities.