DORSET HOUSE SCHOOL

Online Safety Policy

Contents **Page**

Date of policy: February 2017
Reviewed: September 2023
Next review: September 2024

Prepared by: Andrew Owens, Bursar
Approved by: Governors' Estates & Finance Committee

SECTION 1 - INTRODUCTION

It is the duty of Dorset House 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. 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.

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;
- Virtual Reality and Augmented Reality devices and games;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Policy, 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 Policy;
- Staff Behaviour Policy (in Safeguarding Policy);
- Health and Safety Policy;
- Behaviour and Discipline Policy;
- Anti-bullying Policy;
- Retention of Records Policy;
- Taking, Storing and Using Images of Pupils Policy;
- Privacy Notice/Data Protection Policy; and
- PSHEE Policy.

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 Dorset House School we understand the responsibility to educate our pupils on online 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 online safety and listening to their fears and anxieties as well as their thoughts and ideas.

SECTION 2 - SCOPE OF THIS POLICY

This policy applies to all members of the school community, including staff, pupils 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. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

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

SECTION 3 - ROLES AND RESPONSIBILITIES

3.1 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.

3.2 Head and the Senior Management Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. The Head has delegated day-to-day responsibility to the Bursar/online safety coordinator.

In particular, the role of the Head and the Senior Management team is to ensure that:

- staff are adequately trained about online safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

3.3 Bursar/online safety coordinator

The Bursar/online safety coordinator has responsibility for ensuring this policy is upheld by all members of the school community, and works with the external IT contractor to achieve this. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

3.4 IT consultant

The school's external IT contractor 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 will monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Bursar.

3.5 Teaching and support staff

All staff are required to sign the Acceptable Use Policy before 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 online safety issues which may arise in classrooms on a daily basis.

3.6 Pupils

Pupils from Year 3 upwards are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

3.7 Parents and carers

Dorset House School believes that it is essential for parents to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

Parents and carers are responsible for endorsing the school's Acceptable Use Policy.

SECTION 4 - EDUCATION AND TRAINING

4.1 Staff: awareness and training

New staff receive information on Dorset House School's Online Safety and Acceptable Use policies as part of their induction.

All staff receive regular information and training on online 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 online safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. 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.

Teaching staff are encouraged to incorporate online 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.

Staff should inform the Designated Safeguarding Lead and the Bursar if any incident relating to online safety occurs.

4.2 Pupils: e-Safety in the curriculum

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

The school provides opportunities to teach about online 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 PSHEE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHEE, pupils are taught about how to look after their own online safety, about recognising online sexual exploitation, stalking and grooming, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to any member of staff at the school. Pupils can also contact Childline, the Children's Commissioner or the school's Independent Listener. Contact numbers for these are displayed prominently throughout the school.

At age-appropriate levels, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. All pupils are taught about respecting other people's information and images.

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, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach any member of staff for advice or help if they experience problems when using the internet and related technologies.

4.3 Parents

The school seeks to work closely with parents and guardians in promoting a culture of online 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.

The school recognises that not all parents and guardians 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 online 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.

SECTION 5 - POLICY STATEMENTS

5.1 Use of school and personal devices

5.1.1 Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Dorset House School are permitted to bring in personal devices but they must ensure that there is no inappropriate or illegal content on them. Personal use should only take place during break times and when doing so does not interfere with the care or supervision of children.

Staff should not use their personal devices to take photos of children and activities; school devices are to be used. There may, however, be instances where this is necessary, in which case, images must be uploaded to the school network, website or social media sites as soon as possible and then deleted immediately from the personal device. For your own and the children's protection, you should let another member of staff know that you have taken any photos and demonstrate that you have deleted them.

Staff should exercise extreme caution to ensure that images are appropriate. Staff are regularly reminded that there should be no images of children stored on their devices and that this is a serious disciplinary matter and will be regarded as a breach of the staff code of conduct and acceptable use policy. The SMT will, with the permission of the staff member, carry out random spot checks on staff personal devices to ensure that photos are deleted.

Staff should not give their personal mobile phone numbers or email addresses to pupils or ex-pupils, nor should they communicate with them by text message, personal email or social media. Staff may use their personal mobile phones to communicate with parents by text message or phone (e.g. while on a school trip and if there are no alternative means of communication) but should not communicate using personal email or personal social media for school business. Staff may use their own mobile phones to communicate using the school email or social media (e.g. twitter account). The overriding principle is that staff should use their professional judgement and common sense in all communication with parents.

5.1.2 Pupils

No personal devices (mobile phones, smart watches, I-Pads, laptops etc) belonging to pupils, including boarders, are to be used at school, whether for school work or personal use.

The only exception to this is to assist pupils who have disabilities or special educational needs or specific medical conditions that need to be monitored by a mobile app. Where a pupil needs to use a mobile device (e.g. laptop) for such purposes, the pupil's parents or carers should arrange a meeting with the form teacher to agree how the school can appropriately support such use. Devices are to be PAT tested before use.

5.2 Use of internet and email

5.2.1 Staff

Staff must not access any website or personal email which is unconnected with school work whilst teaching/in front of pupils.

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 WiFi are monitored.

Staff must immediately report to the Bursar 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. To ensure against fraud or virus infection, staff must remain alert to the risk of suspicious emails and should report any such emails to the Bursar immediately. Staff should not click on any links or open any email attachments if in doubt.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Dorset House School 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 or ex-pupils be added as social network 'friends' or contacted through social media. Social media contact with parents about school matters should only be via the school facebook, twitter or instagram account.

Any digital communication between staff and pupils or parents/carers must be professional in tone and content. Under no circumstances may staff contact a pupil using any personal email address.

5.2.2 Pupils

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work. Pupils should be aware that email communications through the school network and school email addresses are monitored.

There is strong anti-virus, content filtering and firewall protection on our network.

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 their form teacher.

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 violent or sexual nature directly to their form teacher. 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 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. If this causes problems for school work / research purposes, pupils should contact their form teacher for assistance.

5.3 Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Privacy Notice/Data Protection Policy and the Acceptable Use Policy for further details.

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. Documents should be password protected. No personal data of staff or pupils should be stored on personal memory sticks.

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

5.4 Password security

Pupils and staff have individual school network logins, email addresses 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), which should be changed every six months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5.5 Safe 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, stalking or grooming 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.

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 (e.g. on social networking sites).

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution and publication of those images. Personal equipment, e.g. mobile phones and cameras, may be used to take images for the school social media sites; however, once the images have been uploaded, they should be deleted from personal devices immediately.

Care should be taken that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Parents give written permission when children join the school for images to be published on the school website, media channels and publications. Any parents who wish to opt out are to contact the school office.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

5.6 Misuse

Dorset House School 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 LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the 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.

SECTION 6 - COMPLAINTS

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