DORSET HOUSE SCHOOL

Online Safety Policy

Contents **Page**

Date of policy: February 2017
Reviewed: September 2024
Next review: September 2025

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

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. Online communications and technology provide opportunities for enhanced learning, but also pose great 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 bullying, harassment, grooming, stalking, abuse, radicalization and identity theft.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed within;
- Instant messaging technology via social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

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.

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.

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.).

In designing this policy, the school has considered the "*4Cs*" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk.

3. ROLES AND RESPONSIBILITIES

The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

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. Together with the Senior Management Team, the Head is responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

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

- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise/escalate concerns when identified; 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.

Designated Safeguarding Lead (DSL)

The DSL takes the lead responsibility for Safeguarding and Child protection at Dorset House School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Head, Senior Management Team, Online Safety Co-ordinator and IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSL will take appropriate action if in receipt of a filtering and monitoring report that shows a breach of the school's policies.

The DSL will work closely with the Online Safety Co-ordinator and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review daily filtering and monitoring reports and ensure that regular checks are properly made of the system.

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 Department for Education, ISI, the Local Authority, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. The Online Safety Coordinator also receives a copy of the daily filtering and monitoring reports and will discuss any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

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.

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.

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.

Parents and carers

Dorset House School believes that it is essential for parents to be fully involved with promoting online safety both within 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. Using an external consultant, we organize annual advice sessions for parents on online safety. The school will 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 and carers are responsible for endorsing the school's Acceptable Use Policy.

4. FILTERING AND MONITORING

General

Dorset House School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Coordinator will check once per term that the filtering and monitoring system is operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding governor, the DSL and Online Safety coordinator will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur at least once a year but also if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the Online Safety Coordinator and DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals be identified. In line with the school's Privacy Notice/Data Protection Policy, the DSL and Online Safety Coordinator will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Online Safety Coordinator and the DSL if they are teaching material which might generate unusual internet traffic activity.

Staff

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Safeguarding Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff

should notify the Online Safety Coordinator and the DSL if they believe that appropriate teaching materials are being blocked.

Pupils

Pupils must report any accidental access to materials of a violent or sexual nature or that are otherwise inappropriate to the DSL or appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour and Discipline Policy]. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work, pupils should contact the appropriate teacher for assistance.

5. EDUCATION AND TRAINING

Staff: awareness and training

New staff receive information on Dorset House School's Online Safety and Acceptable Use policies as part of their induction. This includes the school's expectations, applicable roles and responsibilities regarding filtering and monitoring.

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.

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. 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.

In accordance with the Safeguarding Policy, if there is a safeguarding concern relating to an online safety incident, a report must be made by staff as soon as possible to the DSL.

Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular 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 their online safety responsibilities and 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.

Parents

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

6. USE OF SCHOOL AND PERSONAL DEVICES

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.

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.

7. ONLINE COMMUNICATIONS

Staff

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 or parent/carer/ex-pupil using any personal telephone number, email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Pupils and parents should not be added as social network 'friends' or similar.

Staff must immediately report to the DSL or Head 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 Bursar/Online Safety Coordinator.

Pupils

All pupils are issued with their own personal school email addresses for use on our network. 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, assignments and projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work, pupils should contact the appropriate member of staff for assistance.

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 a member of staff who should then refer it to the DSL and the Online Safety Coordinator.

8. USE OF SOCIAL MEDIA

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.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, 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.
- otherwise breach the Staff Code of Conduct or Safeguarding Policy

Pupils

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. The school takes misuse of technology by pupils very seriously and incidents will be dealt with under the Behaviour and Discipline, Safeguarding, and Ani-Bullying policies as appropriate.

9. DATA PROTECTION

Please refer to the Privacy Notice/Data Protection policy and the Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to their school device. Staff devices should be password protected and passwords should be regularly changed.

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, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam/phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the Bursar immediately.

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

10. 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.

11. 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.

12. 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 a member of staff discovers that a child or young person is at risk as a consequence of online activity, they should report it to the DSL. The DSL may seek assistance from the CEOP, the LADO, and/or its professional advisors as appropriate.

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 Safeguarding Policy and Anti-bullying Policy.

13. 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.