

E-SAFETY POLICY

1 Introduction

1.1 Writing and reviewing

This policy takes into account guidance from the DfE (including KCSIE, September 2018), ISI, ISBA and other appropriate organisations. It is published on our school website; further copies are available to parents and students on request.

1.2 Why a policy?

The Internet is a vital tool for modern education; it is an essential part of everyday life for academic work and social interaction both in and out of school. We therefore have a duty to provide students and staff with quality Internet access as part of their learning experience. We also have a responsibility to ensure that, from a young age and as part of their broader education, students understand the inherent risks, and learn how to evaluate online information and how to take care of their own safety and security in the digital world.

Internet use at d'Overbroeck's is intended to enhance and enrich teaching and learning, to raise educational standards and promote student achievement, to develop initiative and independent learning by providing access to information and to alternative viewpoints, to foster imagination and stimulate intellectual curiosity, and to support the professional work of staff and enhance the school's management functions. For boarders, and in particular international boarders, the Internet is, along with the mobile phone, also a crucial means of keeping in touch with home and family.

1.3 Policy Aims

- To enable students to take full advantage of the educational opportunities provided by e-communication;
- To ensure that, as a school, we work to develop in students 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, both in the beyond the classroom.
- To inform and educate students as to what constitutes appropriate and inappropriate Internet usage;
- To safeguard students from potentially harmful and inappropriate online material, including extremist material and ideology, by ensuring that appropriate filtering and monitoring systems are in place;
- To protect students from cyberbullying and abuse of any kind derived from e-sources;
- To help students to understand the range of risks inherent in the digital world – including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse - and to take responsibility for their own online safety;

- To ensure that the copying and subsequent use of Internet-derived materials by staff and students complies with copyright law;
- To clarify the roles and responsibilities of students and staff in these respects;
- To help protect the interests and safety of the whole school community and to provide guidance on how, as a school, we will deal with any infringements.

2 Scope

This policy covers both fixed and mobile Internet devices provided by the school (such as PCs, laptops, tablets, electronic whiteboards, webcams, digital video equipment, etc.) as well as all devices owned by students and staff brought onto school premises (such as personal laptops, tablets, smart phones, etc).

It is linked to a number of other school policies and documents including:

- Safeguarding and promoting the welfare of children
- Anti-bullying
- Behaviour, rules, rewards and sanctions
- Code of conduct for staff
- Data protection
- Acceptable use of IT equipment at school
- Health and safety
- Curriculum and schemes of work for PD (Personal Development) and ICT and the Enrichment Programme

3 Definitions

3.1 **Cyberbullying** can be defined as 'the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others' (Belsey, <http://www.cyberbullying.org/>). It is an aggressive, intentional act carried out repeatedly over time, often against a victim who cannot easily defend himself/ herself.

- Cyberbullying may involve communications by various electronic media, including for example:
 - Texts, instant messages or calls on mobile phones;
 - The use of mobile phone camera images to cause distress, fear or humiliation;
 - Posting threatening, abusive, offensive or humiliating material or comments on websites (including blogs, personal websites and social networking sites such as Facebook, Instagram, Twitter or YouTube);
 - Using e-mail to message others in a threatening or abusive manner; or
 - Hijacking/ cloning e-mail accounts.

3.2 **e-Safety** means limiting the risks to which students and staff are exposed when using the Internet and associated technologies, so that all such technologies are used safely and securely and with a clear understanding of the range of potential risks that could be inherent in their use.

4 Guidelines

4.1 Application

The d'Overbroeck's e-Safety policy applies to day students and boarders. It is interpreted and applied age-appropriately.

4.2 Responsibility for e-safety at d'Overbroeck's

In as much as e-Safety is part of the broader context of Safeguarding, issues relating to e-Safety at d'Overbroeck's fall within the scope of the responsibilities of those members of staff who have designated roles in respect of safeguarding and child protection. They are:

- Emma-Kate Henry (Principal)
- Jonathan Cuff (Deputy Principal), who is the school's Designated Safeguarding Lead (DSL)
- Alasdair MacPherson (Head of Sixth Form)
- Kate Palmer (Head of Lower Sixth)
- Mark Olejnik (Head of Years 7-11)
- Jane Cockerill (Deputy Head of Years 7-11)
- David Wareham (Deputy Head of the International School)

4.3 Student responsibility

Limitations in the provision of hardware (such as filters and firewalls) and the vigilance of teachers and parents have an important part to play in the safeguarding and protection of students both at school and at home. However, young people have wide ranging access to the Internet, so the most effective form of protection ultimately lies in the good sense of young people and in their exercising judgement guided by a well-informed understanding of what is available to them and of the risks to which they are potentially exposed.

For this reason, we work on the basis that students must be responsible for their actions, conduct and behaviour when using the Internet, much as they are responsible during classes or at other times in the school day.

Use of technology should be safe, responsible and legal. Any misuse of the Internet, inside or outside of school, will be dealt with under the school's behaviour policy or, where relevant, the school's Safeguarding policy.

Sanctions will also be applied to any student found to be responsible for any material on his or her own or another website, such as Facebook for instance, that would constitute a breach of school rules in any other context.

4.4 Staff responsibility

All staff working with children have a responsibility to demonstrate, promote and support safe behaviours in their classrooms and to follow school e-safety guidance. The Code of conduct for staff at d'Overbroeck's, which is a part of the Safeguarding policy, contains more detailed information on this.

The school is committed to ongoing professional development for staff that includes online safety.

4.5 **Filtering and monitoring**

The internet has become a significant component of a number of key safeguarding issues including pornography, child sexual exploitation and predation and radicalisation. Schools have a duty and a responsibility to limit children's exposure to such risks on their IT systems.

As part of this process, we have in place a filtering and monitoring system which is designed to comply with the latest government guidance. The system is applied in an age-appropriate way and, in line with the guidance in KCSIE, September 2018, with the aim of ensuring that it does not, through 'over blocking', lead to unreasonable restrictions being imposed on what students can be taught with regards to online teaching and safeguarding.

4.6 **Bullying**

Students must not use their own or the school's devices and technology to bully others either inside or outside the confines of school buildings. Bullying incidents involving the use of technology will be dealt with under the school's anti-bullying policy.

If a student thinks s/he or another student has been bullied in this way, they should talk to a member of staff about it as soon as possible.

4.7 **Abuse**

If there is a suggestion that a student is at risk of abuse from his or her involvement in any form of online activity, including the risk of radicalisation and being drawn to extremist organisations of ideology, the matter will be dealt with under the school's policy for Safeguarding and protecting the welfare of children.

If any student is worried about something that they have seen on the Internet or in a social media context, they must report it to a member of staff about it as soon as possible.

4.8 **Responses**

- All e-safety complaints and incidents will be recorded in the e-Safety Incident Log, together with actions taken.
- Breaches of regulations will be dealt with according to the school's disciplinary and child protection procedures.
- Bullying in any form, including cyberbullying, is wholly unacceptable at d'Overbroeck's. Any instances of cyberbullying will be taken very seriously and dealt with thoroughly and appropriately in accordance with the school's anti-bullying and behaviour rules and sanctions policies.
- In such cases, the Principal or Deputy Principal will apply any sanction that is deemed appropriate and proportionate to the breach including, in the most serious cases, asking a student to leave the school. Misuse may also lead to confiscation of equipment in accordance with the school's policy on behaviour and discipline.
- Where there is reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm as a result of bullying in any form, including cyberbullying, then the matter will be treated as a child protection issue and referred to children's social care as set out in both the school's Anti-bullying and Safeguarding policies.

5 Principles and acceptable use of the internet at d'Overbroeck's

5.1 Password security

Students and staff have individual logins to access the school network, Firefly VLE and storage folders on the server. It is important that staff and students understand and respect the need for complete password security.

All students and staff should:

- Use a strong password, which will need to be changed at regular intervals when prompted by the system;
- Not write their passwords down;
- Strictly never share passwords with anyone else.

5.2 Monitoring and usage

Users should be aware that the school can track and record the sites visited and any searches made on the Internet by individual users.

We would advise parents that we provide filtered access to the Internet for students, but they should also be aware that, with emerging and constantly changing technologies, there is no absolute guarantee that a student will not be able to access material that would be considered unsuitable. The chance of just coming across such content is highly unlikely, but it obviously increases in direct proportion to the amount of time and effort an individual puts into their search.

Anyone inadvertently coming into contact with such material must contact a member of staff immediately.

When using the Internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, data protection, discrimination and obscenity.

Any attempt to access material which promotes extremism or radicalisation will be taken very seriously and dealt with immediately as set out in the section on 'Preventing radicalisation' in the school's Safeguarding policy.

All staff are expected to communicate with students in a professional manner consistent with the guidelines set out in the Code of Conduct for staff at d'Overbroeck's (included in our Safeguarding policy).

Access to the Internet in school is given to students on the understanding that they will use it in a considerate and responsible manner. It may be withdrawn if acceptable standards of use are not maintained.

Staff should ensure that students know and understand that, in addition to the points found in the section on 'Online activities which are not permitted' below, no Intranet or Internet user is permitted to:

- Retrieve, send, copy or display offensive messages or pictures, including sexting and so-called nude selfies;
- Use obscene, racist or otherwise discriminatory language;
- Harass, insult or attack others;

- Access, or attempt to access, material that promotes extremism and or terrorist activity or organisations, pornography or any other form of harmful, inappropriate or illegal content;
- Damage computers, computer systems or computer networks;
- Violate copyright laws;
- Use another user's password or account;
- Trespass in another user's folders, work or files;
- Use the network for commercial purposes;
- Download and install software or install hardware onto a school computer, whether legitimately licensed or not;
- Intentionally waste limited resources, including printer ink and paper;
- Bypass or attempt to bypass any of the school's security or monitoring systems;
- Use the school computer system or the Internet for private purposes unless the Principal or other senior member of staff has given express permission for that use.

5.3 **Online activities which are not permitted in school include:**

- Sending, sharing or in any other way putting on line any content that is racist, discriminatory, pornographic, conducive to extremism, violence or radicalisation, or in any sense offensive to any other person or group of people, including but not limited to protected characteristics under the Equality Act 2010, or likely to bring the school into disrepute;
- Copying, saving or redistributing copyright-protected material without approval;
- Subscribing to any services or ordering any goods or services unless specifically approved;
- Playing computer games unless specifically approved by the school;
- Using Internet chat rooms;
- Using the network in such a way that its use by other users is disrupted (for example: downloading large files during peak usage times; sending mass email messages);
- Publishing, sharing or distributing any personal information about any other user such as home address, email address, telephone number, photographs etc);
- Using school computers or the Internet for financial gain, gambling, political purposes or advertising;
- Any activity that violates a school rule.

5.4 **Managing email**

Email is the *sine qua non* of modern life and an immensely valuable tool for educational communication. However, it can also be a channel for cyberbullying, abuse and defamation. Spam, phishing and virus attachments can also make email dangerous. As a consequence:

- Students may only use approved email accounts on school computers;
- Students must notify a member of staff immediately if they receive offensive email;

- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone not known to them without specific permission;
- Social email use during the school day can interfere with learning and will be discouraged;
- Email sent to external organisations should be written carefully and authorised before being sent, in the same way as a letter written on school headed paper;
- Sending or replying to anonymous messages and chain letters is not permitted;
- Staff should use school email accounts to communicate with students, and such communications must always be professional in tone, content and motivation;
- Staff and students should never click on links received by email unless you absolutely certain you know where the email has originated from. In situations where you are unsure please check with a senior member of staff or with the IT Department by forwarding the email in question to it@doverbroecks.com.

5.5 **Managing social media and social networking sites**

- Parents and teachers need to be aware that the Internet has a host of online spaces and social networks which allow unmediated content to be published. Students should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. Before students share anything online, ask yourself “Is the post kind? Is it true? And is it something I would be happy to be displayed on a large screen in front of the whole school?”
- All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messaging and many others.
- The school will control access to social media and social networking sites because of the potential for harm inherent in such sites, particularly when used by younger pupils.
- Students are advised never to give out personal details of any kind which may identify them and / or their location. Examples include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs, etc.
- Students are advised not to place personal photos on any social network space. They should think about how public the information is and consider using private areas. Tracking and GPS location features in apps such as Snapchat, Twitter, Facebook, Instagram etc. should be turned OFF at all times.
- Staff official blogs or wikis should be password protected. Staff must not run social network spaces for pupil use on a personal basis.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed in how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.

- Students are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Posts that, in the reasonable opinion of the school, could be deemed offensive or defamatory to individuals or to the school will be regarded as a serious breach of discipline and will be dealt with in the context of the school's behaviour policy.

5.6 **Managing mobile phones**

- Students are permitted to bring mobile phones onto school premises, but they remain the responsibility of their owners at all times. The school cannot be held responsible for any theft, loss of, or damage to, such phones suffered on school premises.
- The different sections of d'Overbroeck's have slightly different regulations on mobile phone usage, but common to all sites is the stipulation that such devices must not be switched on or used for any purpose in any lesson or other formal school occasion, unless expressly authorised to do so by a member of staff.
- Students may not bring mobile phones or smart watches into examinations under any circumstances.
- Phones may not be used to bully, harass or insult any other person inside or outside the school either through voice calls, texts, emails, still photographs or videos. Cyberbullying of this nature will bring severe penalties in accordance with the school's behaviour policy.
- Any misuse of the Internet through Internet-enabled phones, such as downloading inappropriate or offensive materials or posting inappropriate comments on social networking sites, will be dealt with in accordance with the school's behaviour policy.
- Phones must not be used to take still photographs or videos of any person on school premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way and should never be posted online.
- Any unacceptable use of mobile phones will be dealt with in accordance with the school's behaviour policy.
- The school reserves the right to confiscate for a fixed period the phone of any person contravening these protocols and to forbid them from bringing a mobile phone into school for any length of time deemed appropriate by the school.

5.7 **Managing photography and video capture on school premises**

- Use of photographic material to harass, intimidate, ridicule or bully other students or staff members will not be tolerated and will constitute a serious breach of discipline.
- Phones must not be used to take still photographs or videos of any person on school premises without their express permission. Even if such permission is obtained they must under no circumstances be used to ridicule, harass, bully or abuse another person in any way.
- Indecent images taken and sent by mobile phones and other forms of technology (sometimes known as 'Sexting') is strictly forbidden by the school and in some circumstances may be seen as an offence under the Protection of Children Act 1978 and the Criminal Justice Act 1988. Anyone found in possession of such images or sending

them will be dealt with by school authorities. If a student thinks that they have been the subject of 'sexting', they should talk to a member of staff about it as soon as possible.

- The uploading onto social networking or video sharing sites (such as Facebook or YouTube) of images which in the reasonable opinion of the school may be considered offensive or harmful is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material. In this context it makes no difference whether the images were uploaded on a school computer or at a location outside of the school.
- Students, if requested, must allow staff reasonable access to material stored on phones and must delete images if requested to do so in any situation where there is any suspicion such images contravene school regulations. (Please see also the policy on Conducting a Search.)
- If it has reasonable grounds to believe that a phone, camera, laptop or other device contains images, text messages or other material that may constitute evidence of criminal activity, the school reserves the right to submit such devices to the police for examination. (Please see also the policy on Conducting a Search.)
- Such misuse of equipment will be dealt with according to the school behaviour policy and may involve confiscation and / or removal of the privilege of bringing such devices into school premises on a temporary or permanent basis.

5.8 **Managing other electronic equipment – eg, laptops, PDAs and tablet computers**

- Students are permitted to bring other electronic devices such as laptops, PDAs, tablet computers and mp3 players onto school premises with permission but they remain the responsibility of their owners at all times. They must keep them with them at all times or in a locked locker and they must ensure that they are appropriately made secure via passwords.
- The school cannot be held responsible for any theft loss of, or damage to, such phones suffered whilst at school.
- No electronic device should be misused in any way to bully, harass or intimidate another person whether through text or images. Any such abuse will be dealt with in accordance with the school's behaviour policy.
- No electronic device should contain inappropriate material such as violent or explicit videos or photographs, pornography or any material that could be considered offensive and / or inappropriate in a school context.
- **Anti-virus software** – all laptops should have appropriate anti-virus software that is regularly updated.
- **Network access** – students may not access the school network from their laptop or any other mobile device without express permission from a member of staff. No student may use another's laptop without permission from that student. Students may also not connect their personal laptops to the Internet via Wi-Fi or Ethernet cable and they are not permitted to connect to any other hardware without express permission. This includes detaching & attaching school keyboards and the mouse for personal use as this renders school equipment inoperable.

- **Licensed software, distributing files / MP3s and Warez** – no computer programmes (executables), MP3s, pornography, copyrighted material or material encouraging radicalisation may be distributed over the network. This includes the sending of files via email, as well as setting up ‘servers’ on students’ laptops and using them as a means of sharing software. Also, students should not download copyrighted material or non-shareware programs and should not be using their laptops as a means to view films, images, or graphics which are deemed inappropriate.
- **‘Chatting’** – students may not use any chat or collaboration program to communicate with others through the school’s computer network unless a member of staff expressly permits them to do so. This includes the use of email during lessons.
- **Audio** – because computer audio can be distracting, the volume setting on laptops must generally be turned off when used during school time.
- **Games** – computer games should never be played in class, during study time, lunchtime sessions or in after school clubs unless part of a specified homework that is detailed in the student planner or on Firefly. These should be age appropriate and not contain offensive material in the form of images, sounds or graphics. These will be checked by a member of staff. Students will be asked to remove them if they are deemed inappropriate.
- **Privacy** – the school reserves the right to examine the hard drive on a student’s personal laptop if there is reasonable suspicion that a computer is being used for inappropriate or dishonourable purposes.
- **School owned laptops / netbooks** – these must only be used under the supervision of a member of staff and must only be used for educational purposes. The uploading of inappropriate material such as images, software and graphics is forbidden, and this includes the doctoring of screen savers and backgrounds.
- **Consequences** – students found in breach of these rules may have their Internet privileges removed, the privilege of using their laptop, netbook, PDA or tablet PC at school removed either permanently or temporarily, and, depending on the seriousness of the breach, they may also have other sanctions imposed in accordance with school’s behaviour policy.

6 Responses to cyberbullying

- Please see the definition of cyberbullying given in section 3.1 above.
- Many young people and adults find using the Internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobile phones, gaming or the Internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.
- It is essential that students, staff and parents understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.
- The DfE and Childnet have produced resources that can be used to give practical advice and guidance on cyberbullying. See: <http://www.digizen.org/cyberbullying>

- Cyberbullying (along with all forms of bullying) will not be tolerated at d'Overbroeck's, whether the bullying originates inside or outside school. Activities conducted outside of school premises and outside of school hours that in our opinion constitute cyberbullying will also be covered by this policy. Instances of cyberbullying will be dealt with according to the school's anti-bullying policy or, where relevant, the school's Safeguarding policy. All incidents of cyberbullying reported to the school will be recorded.
- The school will take reasonable steps to identify the person(s) responsible for any instances of cyberbullying such as examining system logs, identifying and interviewing possible witnesses and contacting the service provider and the Police if necessary.
- Sanctions may include: Informing parents/guardians, the withdrawal of privileges, eg, to bring a phone into school or to use the school Internet facilities, the person(s) responsible being instructed to remove any material deemed to be inappropriate, temporary or permanent exclusion in the most serious cases, and the Police being contacted if a criminal offence is suspected.

Sources:

Keeping Children Safe in Education (KCSIE), September 2018

'Preventing and tackling bullying - advice for headteachers, staff and governing bodies', October 2014

ISI guidance

e-safety guidance and model policy issued by the ISBA

Becta www.becta.org.uk/safeguarding

Bristol LA's NGfL Learning Project

CEOP (Child Exploitation and Online Protection Centre www.ceop.police.uk)

*

Last reviewed: August 2018