



All policies carrying the Bryanston logo apply to any other brands or operations of Bryanston including Bryanston Prep

Author:	Digital Wellbeing & Online Safety Lead (DDSL)
Reviewer:	Senior Deputy Head (DSL)
Reviewed:	September 2025
Next Review:	September 2026

DIGITAL ONLINE SAFETY AND CYBER BULLYING POLICY

It Is Essential That You Read And Understand This Policy.

Safeguarding young people at Bryanston School is taken very seriously. In the School's Safeguarding policy it is clear that as a school we are committed to creating and sustaining a safe learning environment and identifying that where there are child welfare concerns, we take swift and informed action to address.

This policy is split into two sections:

1. Digital Online Safety.

- Outlining our practices regarding responsibilities, systems, equipment, communication, and advice.

2. Cyber-Bullying.

- Outlining our expectations, sanctions, and The Anti-Cyber Bullying Code.

Section 1: Digital Online Safety

Background and Rationale

All staff at Bryanston are trained to understand and appreciate that everyone has a duty to safeguard and promote the welfare of children – and not just those children at Bryanston school. [Keeping Children Safe in Education \(2025\)](#) defines safeguarding as “*protecting children from maltreatment; preventing impairment of children’s mental and physical health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.*”

The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is a vital part of the wider duty of care to which all who work at Bryanston are bound. A school digital online safety policy should help to ensure safe and appropriate use of technologies, both within and outside of the classroom.

The development and implementation of such a strategy should involve all the individuals in a child’s education from the Head and Governors to the Executive Leadership Team and teachers, non-teaching



staff, parents, members of the community and, most importantly, the pupils of Bryanston themselves. New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other.

We have introduced single devices (Apple iPad) to the classrooms to support increased organisation and standardise learning approaches where applicable. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. However, it must also be remembered that children and young people have an entitlement to safe internet access at all times. Whilst the use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include ([KCSIE 2025](#)):

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact:** being subjected to harmful online interaction with other users; for example: 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:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies such as the *ICT policy*, *Anti-Bullying policy*, *Child-on-Child Abuse policy* and *Safeguarding and Child Protection policies*. As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. Bryanston School also believes that through education, open conversation and early intervention through alerting tools, we will encourage our young people to discuss any issues or challenges they are facing online and ask for help and/or support where appropriate.

Bryanston aims to demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. Underpinning the following online safety policy are the frameworks and Government legislation set out in '[Keeping children safe in Education](#)' (2025), '[Working together to Safeguard Children](#)' (2018, updated Dec 2023) and the DfE document '[Meeting Digital and Technology Standards in Schools and Colleges](#)' (2025) and "[Sharing of nudes and semi-nudes: advice for education settings working with children and young people](#)" (DfE 2020, updated May 2024). If students or staff are at risk, reports can be made to the Anti-Phishing Working Group (<https://apwg.org/>). The policy that follows explains how we intend to manage the risks mentioned above, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.



This policy has been reviewed by:

- **Senior Deputy Head**
- **Online Wellbeing & Online Safety Lead / DDSL**
- **Safeguarding Co-ordinator**
- **Director of IT Development and Services**
- **Digital Safety and Systems Officer / DDSL**

Information regarding the policy is shared with the whole school community through the following channels:

- Staff meetings
- Bryanston SharePoint sites – StaffHub and PupilHub
- Governors' meeting / subcommittee meetings (Wellbeing & Safeguarding Committee and Child Protection Advisory Committee)
- Information sharing via the Parental Online Committee
- Student Voice groups
- House Parent weekly meetings

The policy will be reviewed annually by the Governors alongside the Safeguarding and Child Protection policy. This will be overseen by the Deputy Head responsible for safeguarding.

Any changes to the policy (due to legislation changes or considering any significant new developments in the use of technologies, new threats or online safety incidents that have taken place) will be clearly identified. Should any serious incidents take place, the Designated Lead for Safeguarding will be informed and communication with Children's Social Care or the LADO if appropriate.

Scope of the Policy

This policy applies to all members of the Bryanston community (including staff, pupils, volunteers, parents, visitors) who have access to and are users of school ICT systems, both in and out of school. This applies to everyone who accesses the network, any software products and services and all school issued and owned devices. The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. This may include, for example, instances of where cyber bullying have taken place over the summer holidays and has continued into term time or if a pupil has brought the school into disrepute over social media using a personal device, or from their home. The school will deal with such incidents within this policy and associated behaviour and child-on-child abuse policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school. Additional information about cyberbullying can be located in Section 2 of this policy.



Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the School:

The Head and School ExCo: The Head is responsible for ensuring the safety of the members of the school community, though the day-to-day responsibility for online safety will be delegated to the Senior Deputy Head, Deputy Head (Boarding & Pastoral), DDSL (Digital Wellbeing & Online Safety Lead) and the Safeguarding Co-ordinator.

The Head and the ExCo alongside the Deputy Head (Boarding & Pastoral) are responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant

The Head and the ExCo alongside the Deputy Head (Boarding & Pastoral) will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

The Senior Deputy Head, Deputy Head (Boarding & Pastoral), DDSL and Safeguarding Co-ordinator will also review any online safety incidents and discuss them, addressing what had been done well and what could have been done better. In accordance with the School's ethos, an undefended and reflective approach will be taken.

Should a member of staff need any support following an online safety incident, the Deputy Head (Boarding & Pastoral) will ensure that appropriate support be given to that individual and confidential counselling offered if needed via the HR team and the employee assistance service

Leadership of Online Safety

The Senior Deputy Head takes responsibility for online safety within the School working alongside the Director of Digital, Data & Technology (DDaT), the DDSL and the Safeguarding Co-ordinator. They will meet at least termly to look at any aspects of online safety that need to be addressed, however it is expected that informal liaison will take place on a much more regular basis and as and when required.

The Senior Deputy Head will act as main point of contact on online safety issues and liaise with other members of staff as appropriate. They will in conjunction with the DDaT, ensure policies and procedures that incorporate online safety concerns are in place. This should include but is not limited to.

- Safeguarding & Child Protection
- ICT Acceptable Use
- Mobile phone policy
- Child on child abuse (including responses to cyberbullying and the sharing of nude and semi-nude images) and social media.



The Senior Deputy Head, Safeguarding Co-ordinator and Digital Wellbeing Lead will:

- Ensure there are robust reporting channels (via MyConcern and Whisper) and signposting to internal, local and national support.
- Record online safety incidents and actions taken, in accordance with Bryanston's Safeguarding & Child Protection policy.
- Ensure the whole school community is aware of what is safe and appropriate online behaviour and understand the sanctions for misuse.
- Liaise with the local authority and other local and national bodies as appropriate.

There will be a newly created online safety group which includes the Deputy Head (Boarding & Pastoral), a member of the House Parent team, the DDSLs and the DDaT, who will work together to develop an online safety curriculum where appropriate and inform technical decisions across monitoring/alerting and filtering. This group's remit will be to:

- Produce and review policies.
- Map, plan and review the online safety curriculum where applicable.
- Establish, review and monitor the school monitoring and filtering policy.
- Raise awareness throughout the community of the importance of being safe online.
- Audit online safety practice and policy compliance.
- Create and implement an online safety action plan if needed.
- Report regularly to the governing body to help inform them of existing practice and localised concern.
- Keep the Head regularly informed of any incidents and concerns and take responsibility for implementing actions as appropriate, liaising with the Assistant Head Pupils over disciplinary decisions.
- Work to ensure that appropriate filtering and monitoring is in place and that the DfE standards for filtering and monitoring are being met
- Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern.
- Work with Head of Compliance to ensure that online practice is in line with current GDPR legislation.
- Implement regular online safety training for all members of staff (including as part of induction) that is integrated, aligned and considered part of the overarching safeguarding approach.
- Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum, promoting the responsible use of technology and empowering children to keep themselves and others safe online.

The group will also endeavour to ensure that online safety is promoted to parents, guardians and carers and the wider community through a variety of channels and approaches, including the Friday Flyers, tutor conversations, social media channels.

The group identified must ensure that their own knowledge and skill are refreshed at regular intervals to enable them to keep up to date with current research, legislation and trends in order to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school.



The group are also tasked with evaluating and ensuring the delivery and impact Bryanston's online safety policy and practice. This may include reviewing any reported online safety incidents to inform and improve future areas of teaching, training and policy development.

The Director of Digital, Data & Technology and the Digital Safety and Systems Officer are responsible for ensuring that:

- the School's ICT infrastructure is secure and is not open to misuse or malicious attack
- users may only access the School's networks through a properly enforced password protection policy, in which passwords are monitored and updated where necessary
- the newly formed Bryanston filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- they keep up to date with e-safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- the use of the Virtual private networks / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the for investigation / action / sanction
- monitoring software / systems are implemented and updated as agreed in School ICT policies
- they liaise with the Senior Deputy Head, DDSLs, Safeguarding Co-ordinator and House Parent teams with any concerns

The teaching and support staff are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices including an understanding of the filtering and monitoring processes in place and what is allowed within the School's ecosystems.
- They have read, understood and signed the School ICT policy and the Online Safety policy.
- They report any suspected misuse or problem (for example failure to comply with the conditions of the ICT policy) to the Senior Deputy Head for investigation / action / sanction (any decision of which will be made in conjunction with the Head and ExCo)
- Digital communications with students (email/Virtual Learning Environment (VLE)/voice) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the School's Online Safety and ICT policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations as per the academic integrity policy
- They monitor ICT activity in lessons, extracurricular and extended school activities, recognising that pupils using mobile phones may be using their own data access and not the School's Wi-Fi.
- They are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies regarding these devices, especially regarding pupils using their own data plans to access the internet.
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches, blocked via firewalls or flagged through altering software.
- They celebrate the positive use of ICT and digital media and promote correct usage



The Senior Deputy Head together with the DDSL Digital Wellbeing & Online Safety lead have overall responsibility for online safety within the School and should be trained in online safety issues, including understanding the filtering and monitoring systems and processes in place, and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying

They should liaise with Children's Social Care and the LADO when appropriate

The Senior Deputy Head has regular meetings with the DDSLs, and online safety team outlined above to keep the safeguarding team abreast of online safety issues both nationally and within the School.

Pupils are responsible for using the School ICT systems in accordance with the ICT policy, which they will be expected to sign before being given access to school systems and is shared ahead of any pupil joining the School. They are also expected to:

- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so either to an adult, through Whisper or sharing with a peer.
- Will be expected to know and understand school policies on the use of mobile phones, single devices and the network.
- They should also know and understand school policies on the taking / use of images and on cyber-bullying, code of conduct.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety policy covers their actions out of school, if using a school issued device.
- They must understand how to use mobile devices in an appropriate way.

Research shows that many parents, guardians and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The School will therefore take every opportunity to help parents understand these issues through:

- Sharing information advice in Friday Flyers, discussions through our tutoring system, letters home, and information about national/local e-safety campaigns/literature.
- Parents also need to be aware that if their children are supplied with a 3G/4G/5G mobile device they will be able to access the internet independently of the Bryanston's network and systems and therefore the School's blocking and filtering system will not operate whilst these devices are being used on the 3G/4G or 5G networks.
- This further highlights the need for parents, guardians and carers to take responsibility for educating their own children in digital technology and social media alongside the work that Bryanston undertakes.



Parents, guardians and carers will be responsible for:

- Ensuring that they are well educated themselves on all matters of online safety. Parents are strongly encouraged to engage with the support material that Bryanston will provide over the course of the academic year.
- Supporting the School's actions within online safety if action has been taken, and an issue has been dealt with.

Children and young people need the help and support of the School to learn about online safety and to recognise and avoid online safety risks and build their resilience. Online safety education will be provided in the following ways:

- All pupils will sign the ICT policy at the start of their Bryanston journey.
- A planned online safety programme is provided as part of the PSHE curriculum.
- The content of lessons and talks will be regularly reviewed so that they are up to date and relevant.
- The DSL will, through start of year talks, highlight the issue of the sending of nudes and semi-nude images to all pupils so that they are fully aware of the legal implications of images and the fact that the image may be considered indecent.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the secure use of online tools and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- They should also be educated about protecting their own devices (such as password protecting their mobile and tablets).
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in ICT/online safety / health and safety / child protection. This may be offered by:

- Safeguarding Governor training
- Participation in school training / information sessions for staff
- Membership and access to National Online Safety platform courses/guides/webinars

Technical – Infrastructure / Equipment, Filtering and Monitoring

Bryanston will be responsible for ensuring that the School infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The School will also ensure that it meets the standards as laid out in the DfE document 'Meeting digital and technology standards in schools and colleges' (March 2023). It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:



- There will be regular reviews and audits of the safety and security of school ICT systems. This will be covered in meetings between the Senior Deputy Head and the DDaT and IT Services team. These audits and any action points will be shared with the ExCo.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the DDaT and IT Services team and will be reviewed, at least annually.
- All users will be provided with a username and password by IT Services who will keep an up-to-date record of users and their usernames.
- Users will be required to have a robust password.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The School has provided enhanced user-level filtering through the use of the Darktrace Firewall and Lightspeed filtering and monitoring system. The specific software used for this process is kept under review as other products and systems become available.
- In the event of the DDaT needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is established and agreed
- Requests from staff for sites to be removed from the filtered list will be considered by the DDaT in line with Bryanston's code of conduct and ICT policies.
- School IT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the ICT policy.

Monitoring will take place across both staff and student account.

Emails in particular will be read to and checked for:

- General inappropriate language – overtly disciplinarian or affectionate. Anything which suggests an uncomfortable power imbalance between the adult and the child such as threatening or intimidating language or anything which suggests a relationship which might be too close such as flirtatious language.
- Pupil language – general email etiquette and the way in which they are engaging with the member of staff. All email contact needs to be 'professional'. All emails should be professional in their tone and content.
- Inappropriate conduct – including personal mobile phone numbers, personal email details or home address or social media contact details. Organising to meet a pupil in an inappropriate place / time. Same to be looked for in pupil emails.
- Context – has an email been sent when a different method of communication would have been better? Is there some education to be done with staff / pupil?

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are kept secure via a number of initiatives:

- The School infrastructure and individual workstations and school-issued devices are protected by up-to-date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.



Curriculum Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Where pupils are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring (via JAMF or Apple Classroom) the content of the websites the young people visit by continually moving around the classroom and engaging with the pupils throughout the lesson and in assignment periods or prep, staff should be aware that pupils may be using mobile phones or mobile data to bypass technical security settings.

It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request, via esupport, that they can temporarily remove those sites from the filtered list for the period of study. Any request to do so should also be cleared by the HoD in the related subject and a ticket raised with IT.

Pupils should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information, with particular focus on scamming and changes in cyber-crime. Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of Digital and Video Images - Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate 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.
- Staff are allowed to take digital / video images to support educational aims but must follow school policy concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment; the personal equipment of staff should not be used for such purposes. If a member of staff wants to use their own equipment, they need the permission of the Senior Deputy Head.



- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the School into disrepute. If in doubt, the individual should ask the advice of the Senior Deputy Head.
- Pupils must not take, use, share, publish or distribute images of other pupils without their permission. It must be recognised by the pupils that these permissions can change depending on the relationship between particular groups of pupils. Permissions to use or not to use images can be given verbally.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. The School's Terms and Conditions clarify what is permissible and parents are required to opt out of the sharing of such images when signing the Bryanston contract. Any images which are published should be without the name of the individual pupil (unless permission has been agreed by the pupil and their parent).
- Particular care should be taken in subjects such as Art, where it may be necessary for pupils to capture images using digital media of semi-naked models as part of their portfolio work. Advice should be sought from the Senior Deputy Head if there are any concerns.
- Pupil's work can only be published with the permission of the pupil.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they are fully conversant with Bryanston's Data Protection policy. In the context of online safety, they should:

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices. When personal data is stored on any portable computer system, USB stick or any other removable media:
 - It is good practice to password protect the device.
 - The device must offer approved virus and malware checking software.
 - The data must be securely deleted from the device, once it has been transferred or its use is complete.



Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. When using communication technologies, the School considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and pupils should therefore use only the School email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to the Senior Deputy Head and can also report such an incident using the Whisper confidential reporting app, which is monitored closely.
- The recipient must not respond to any such email. If the recipient is a pupil, they should inform any member of staff although it is likely that they will speak to their House Parent in the first instance. The email should be printed and saved before any further action is taken. Any digital communication between staff and pupils or parents/guardians/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Information on the school social media channels will be uploaded by the designated member of staff and content is monitored.

Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Personal information should not be posted on the School website and only official email addresses should be used to identify members of staff. The Bryanston Safeguarding and Child Protection policy and Staff Code of Conduct details the School's policy on the staff use of mobile phones.



Unsuitable / inappropriate activities which will result in actions/sanction

The School believes that the activities referred to in the following section would be inappropriate in a school context and that all users of the School IT system should not engage in any of the following activities in school or outside school when using school equipment or systems:

- Child sexual abuse images as laid out in statutory law (<https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children>)
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in the UK
- Pornography
- Promotion of any kind of discrimination, racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the School or brings the School into disrepute
- Using school systems to run a private business
- Use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling should not be used by any of the pupils in school or outside school when using school equipment or systems. It should be remembered that gambling is illegal under the age of 18.

Responding to incidents of abuse

- It is assumed that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Any such incidents should be reported to the Senior Deputy Head or HR.

All staff are reminded that there is a clear Bryanston Whistleblowing policy (accessed from the main policies link on MyBry) which they should refer to if required.



Remote Learning

Bryanston remains committed to staff and pupils embracing the use of technology to support teaching and learning across the School. It is important to ensure that appropriate use supports the core values of the School and does not undermine the importance of developing strong interpersonal communication. These guidelines in this policy aim to promote safe, respectful, and responsible use of online tools and devices to the benefit of the whole community.

The following guidance is to ensure that pupils are safeguarded, and staff are protected whilst learning either at school or remotely

Technology

Bryanston's policy is for Microsoft Teams to be used for all remote video conferencing. Microsoft Teams has been selected due to many considerations such as being able to use school email accounts, the safeguarding of personal data, privacy questions and policies and terms of service. By deciding to use another means of communication, the relevant checks and safeguarding measures may not have been put into place, therefore, you should avoid changing platforms if communication is disrupted by technical difficulties; reschedule the session instead.

The usual safeguarding and ICT information applies in addition:

- Do not post or 'broadcast' anything which will bring you or Bryanston into disrepute.
- Use only school provided equipment and do not use personal devices. If circumstances arise which necessitate you using a personal device (such as your Bryanston device breaking), you must inform the DSL and seek support from ICT.

Reporting

Any safeguarding incidents / concerns should be reported to the DSL as soon as possible so that advice and support can be given. The DSL will log any such occurrences as a self-report.

If there are issues over pupil behaviour during a video conferencing lesson, this should be reported to the Deputy Head (Academic).



SECTION 2: CYBERBULLYING

General

Cyberbullying may be defined as *'the use of Information and Communications Technology (ICT), particularly mobile phones and the Internet, to deliberately upset someone else'*. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. In many ways features of cyberbullying replicate aspects of bullying. However, it does differ in several significant ways from other types of bullying: the potential invasion of home and personal space, the difficulty in controlling electronically circulated messages, the potential size of the audience and the perceived anonymity which is often involved.

Cyberbullying may take different forms, including threats and intimidation, harassment or 'cyberstalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images. (Please refer to Bryanston School Child-on-Child Abuse Policy).

Some cyberbullying is clearly deliberate and aggressive, but it is important to recognise that some incidents of cyberbullying may well be unintentional and the result of simply not thinking about the consequences. What may be sent as a joke may not be received as one, and indeed the distance that technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy. Pupils need to be aware of the effects of their actions.

In many cases of cyberbullying, bystanders can easily become perpetrators, e.g. by passing on or showing to others, images designed to humiliate, or by taking part in online polls or discussion groups. Such people may not recognise themselves as participating in bullying, but their involvement has the potential to compound the unhappiness for the person being targeted. 'Bystanders' or 'accessories' who actively support cyberbullying are liable to face sanctions themselves. Pupils who become involved in this respect need to be aware that their actions may have severe and distressing consequences, and that participating in such activity will not be tolerated.

There are particular features of cyberbullying that differ from other forms of bullying. The key differences include:

- **Impact:** the scale and scope of cyberbullying can be greater than other forms of bullying.
- **Targets and perpetrators:** the people involved may have a different profile to traditional bullies and their targets.
- **Location:** cyberbullying may take place on a "24/7 basis" and, given the nature of electronic communication, its effects may be felt in any location.
- **Anonymity:** the person being bullied will not always know who is attacking them.
- **Evidence:** unlike some other forms of bullying, the target of the bullying is likely to have evidence of its occurrence.



Different Technologies

Cyberbullying may take place through any of the following electronic media:

- Mobile phones
- Instant Messenger and Voice over Internet Protocols
- Chat rooms and message boards
- Email
- Webcam
- Social media platforms
- Video hosting sites
- Virtual learning environments
- Gaming sites, consoles and virtual worlds
- Blogs and Wikis

Prevention

The School has a clear Anti-Bullying Policy Statement which seeks to reinforce values in all members of the School, which should, ideally, preclude all sorts of bullying, including cyberbullying. In addition to this general statement, this statement on cyberbullying has been produced in order to address features specific to cyberbullying. All aspects of bullying, including cyberbullying, are addressed in the PSHE programme. There are also year group talks delivered by external speakers and by the Deputy Head Pupils/Digital Wellbeing & Online Safety safeguarding lead. In addition, there are specific assemblies, both School and House-based, which seek to deal with aspects of cyberbullying. Furthermore, staff are trained in e-safety, which includes cyberbullying.

It is important that all members of the School community are aware that cyberbullying is unacceptable and should not be tolerated. It is the responsibility of all members of the community to take action if they are aware of cyberbullying taking place; to remain silent could be seen as condoning the action of the bully. The School will also seek to build resilience in its pupils to protect them and their peers through education (PSHE, Assemblies, House Assemblies, etc). When cyberbullying is investigated, reference will be made to the School's Digital Communications Policy. The School has, through the Digital Communications Policy, procedures in place to actively manage hardware and software connectivity within the school setting. The filtering system is managed by the Digital Safety and Systems Officer and maintains regular contact with the Senior Deputy Head (DSL), Deputy Head Boarding & Pastoral (DDSL) and the Deputy Head Pupils (DDSL) in relation to safeguarding matters.

Communication takes place with parents advising them about e-Safety, and information sessions are arranged in conjunction with the Bryanston Parents' Association in this regard.

Cyberbullying takes many forms and may cover physical appearance, disability, nationality, race, gender, religion and sexual orientation.



What should a pupil do?

1. If a pupil receives an email or text (or any other form of unacceptable electronic communication), that might be considered to be cyberbullying, they should report the matter to a member of staff (usually the House Parent) as soon as possible. A copy of the electronic communication, plus dates and times should be saved wherever possible.
2. Depending on the nature of the allegation, the case will usually be addressed initially either by the House Parent or by the Assistant Head Pupils. For more serious allegations, the incident will certainly involve the Senior Deputy Head and, in extreme cases, could involve the Police or other external agencies.
3. Pupils involved will be interviewed and given the opportunity to state their case, in order to establish the truth in what seldom turns out to be straightforward issues. The investigation may also involve the Digital Safety and Systems Officer who may have access to various electronic records. In all cases, pupils will be warned not to do or say anything that may prejudice their position vis-à-vis the pupil who has been bullied.
4. At the conclusion of the investigation, and in the light of what has been concluded, the outcome will be announced. This will be communicated to the staff and pupils involved and to parents. As indicated below, there is a range of sanctions which may be applied.

Education

We seek to achieve these aims through a whole School approach, which is principally based on delivery via the PSHE programme and in IT lessons, but also in other contexts (including School assemblies and House assemblies).

Sanctions

Sanctions applied may range from a restorative conversation or a verbal warning to one of the School's standard punishments (i.e. Detention or Chart), even ranging up to temporary or permanent exclusion, depending on the gravity of the offence and the pupil's record with reference to bullying.

The aim of sanction is to:

- Help the person harmed to feel safe again and be assured that the bullying will stop.
- Hold the perpetrator to account getting them to recognise the harm caused and to deter them from repeating the behaviour.
- Demonstrate to the School community that cyberbullying is unacceptable and that the School has effective ways of dealing with it, so deterring others from behaving similarly.



Anti-Cyberbullying Code: Advice to pupils

This section is intended to help pupils protect themselves from getting caught up in cyberbullying and to give advice about how to report it when it does happen. Seeing inappropriate comments about oneself on a website or being sent abusive or threatening text messages can cause considerable upset.

1. Respect other people

Remember that when you send a message to someone, you cannot see the impact that your words or images may have on the other person. That is why it is important to always show respect to people and be careful what you say online or what images you send. What you think is a joke may really hurt someone else. Always ask permission before you take a photo of someone.

If you receive a rude or nasty message or picture about someone else, do not forward it. You could be assisting a bully and risk being accused of cyberbullying. You could also be breaking the law.

2. Think first before you send

It is important to think before you send any images or text about yourself or someone else by email or mobile phone, or before you post information on a social media site or website. Remember that what you send can be made public very quickly and could stay online forever. Parents, teachers, friends or future employers may be able to access photos in years to come.

3. Protect your password

Take care to ensure that other people do not know your passwords. It is a good idea to change them on a regular basis, and you are advised not to use obvious passwords like your name or date of birth. Choosing hard-to-guess passwords with symbols or numbers will help stop people hacking into your account and pretending to be you. It is also sensible to give your mobile phone number only to trusted friends.

4. Block the Bully

Most responsible apps, websites and services allow you to block or report someone who is behaving badly.

5. Do not retaliate or reply

Replying to bullying messages, particularly in anger, may well be what the bully wants and can easily escalate matters very quickly.

6. Save the evidence

It is important to keep records of offending messages, pictures or online conversations. If you are intending to make a complaint, this will help you demonstrate to others what is happening and can be used by the School, Internet Service Provider, mobile phone company, or even the Police to investigate the cyberbullying.

7. Make sure you report incidents of cyberbullying

You have a right not to be harassed and/or bullied online and you should report incidents of cyberbullying which take place.



There are people who may be able to help:

- You should tell your House Parent, Tutor, the Assistant Head Pupils or any other member of staff, who will be able to advise you on this.
- The provider of the service you have been bullied on (e.g. your mobile-phone operator or social network provider). Check their websites to see where to report.
- If you are unable to make progress with the areas listed above, you are able to call a helpline, such as Childline on 0800 1111.

Finally, it should be kept in mind that the School may take a view upon any items published, by any means, if those items could bring the name of the School into disrepute. This is not confined to term-time only.

The School understands its responsibilities in relation to cyberbullying by undertaking the following:

- (a) Clearly defined roles and responsibilities for online safety as part of the School's wider safeguarding strategy and how this links with other safeguarding policy.
- (b) Clear guidance on the use of technology in the classroom and beyond for all users, including staff, pupils and visitors that references permissions/restrictions and agreed sanctions.
- (c) Detail the School's technical provision/infrastructure and the safeguards in place to filter and monitor inappropriate content and alert the School to safeguarding issues.
- (d) Detail on how the School builds resilience in its pupils to protect themselves and their peers through education and information.
- (e) Detail on staff safeguarding professional development that includes online safety.
- (f) Reporting mechanisms available for all users to report issues and concerns to the School and how they are managed and/or escalated.
- (g) How the School informs, communicates with and educates parents/carers in online safety.
- (h) The management of personal data in line with statutory requirements.



Appendix 1:

Remote Learning Guidelines (Teacher)

1. When conducting a one-to-one video conference (via Teams) with a student it is important that you have checked the following:
 - (a) You have invited another member of staff to a video conference you are conducting with a student/s. This may be the student's house parent, tutor or DSL on duty during holiday periods. It is the invite (visibility of the meeting occurring) that is important here not their attendance in the video conference.
 - (b) You have invited students and staff using their school email address.
 - (c) Your background is free of unwanted imagery and personal affects. It is best practice to blur your background.
 - (d) You are dressed appropriately. Your language and tone must always be professional and appropriate.
 - (e) Consider recording the session in order to protect you and the student/s.
2. Situations to avoid online and which may blur communication boundaries between you and the student are:
 - A casual and intimate atmosphere
 - Intimate locations
 - Casual and inappropriate dress
 - Nicknames vs preferred iSAMs
 - Private conversations
 - Observational comments about home or family
 - Oversharing personal details
3. Doing the following is a breach of the Bryanston ICT policy and disciplinary action will be taken:
 - Taking photos or screen shots of students
 - Derogatory remarks
 - Being under the influence of alcohol or drugs whilst conducting a video conference call

Video Conference Call for Remote Learners

1. As a rule of thumb, if pupils are absent through illness, they should prioritise getting better. If they are too ill to attend school, they should not be accessing lessons on Teams.
2. In cases where the pupil is absent but is perfectly able to concentrate or is worried about getting behind (e.g. recovery from a broken limb), it is up to the teacher whether it is beneficial for that pupil to attend lessons via Teams. For example: if material is being explicitly taught, that would be a good lesson to attend virtually.
3. In these exceptional circumstances, House Parents will inform teachers when a student is in a situation where they would benefit from attending lessons virtually. Arrangements should be made in liaison with both House Parent and Tutor.
4. Pupils should be invited to timetabled lessons via Microsoft Teams either by 'Schedule a meeting' or clicking the 'Meet now' button at the start of a lesson.



5. There is no requirement for you to record the lesson.
6. Keep a record of whether or not the pupil attends the lesson.
7. Ensure the student is able to view any shared content, e.g. PowerPoint, by sharing your screen and ensuring OneNote is up to date.

Guidance for Pupils and Parents

Whilst the above guidance is relevant to parents, carers and pupils, please note the following points:

1. When pupils are participating in a video conference or accessing lessons online, they should be in an environment which, where possible, is public and free from distractions.
2. Pupils should be dressed appropriately, adhering to standard classroom expectations.
3. Pupils should not record the lesson/video conference.
4. Pupils should not share the video of the lesson/video conference with anyone without having received the express permission from the member of staff taking the lesson/conducting the video conference. Any breach will invoke a disciplinary response