BELVEDERE
PREPARATORY SCHOOL

ONLINE SAFETY POLICY
2023-2024

REVIEWED: OCTOBER 2023

MISS C. BURNHAM (HEADMISTRESS)
MS A. JONES (DESIGNATED SAFEGUARDING LEAD)
MISS O. GINGELL (ONLINE SAFETY LEAD)
MISS A. SPENCE (CURRICULUM LEAD)
MR J. SHARPLES (COMPUTING LEAD)
MS S. CLARKE (PHSe LEAD)
MISS G. THOMPKINS (AABYSS)
MRS K. CURRIE (DESIGNATED SAFEGUARDING BOARD MEMBER)

UPDATED: OCTOBER 2023
DATE FOR REVISION: JANUARY 2024

ANNUAL REVIEW: OCTOBER 2024

Schedule for development Monitoring and Review

This Online Safety Policy was approved by the *school governing body on:*	*October 2023*
The implementation of this Online Safety Policy will be monitored by:	*Designated Safeguarding Lead, Online Safety Lead, Senior Leadership Team,*
Monitoring will take place at regular intervals:	*Annually*
The *Management Board* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	*Termly*
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be: *January 2024*	*September 2024*
Should serious online safety incidents take place, the following external agencies should be informed:	safeguarding@belvedereprep.com Call the police if appropriate: 0151 709 6010 or 999

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
  learners
  staff
  parents

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups.

Contents

1. Introduction

This Online Safety Policy outlines the commitment of The Belvedere Preparatory School to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

The Belvedere Preparatory School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents/carers, where known, if incidents of inappropriate online safety behaviour that take place out of school.

2. Policy Aims

2.1 The aim of this policy is to promote and safeguard the welfare of all pupils through the implementation of an effective online safety strategy which:

- protects the whole School community from illegal, inappropriate and harmful content or contact;
- educates the whole School community about its access to and use of technology; and
- establishes effective mechanisms to identify, intervene and escalate incidents where appropriate.

3. Scope and Application

3.1 This policy outlines the commitment of The Belvedere Preparatory School to safeguard members of our School community online in accordance with statutory guidance and best practice.

3.2 This policy applies to the whole School including the Early Years Foundation Stage (EYFS).

4. Regulatory framework

4.1 This policy has been prepared to meet The Belvedere Preparatory School's responsibilities under:

Education (Independent School Standards) Regulations 2019;

Statutory framework for the Early Years Foundation Stage (DfE, March2021);

Education and Skills Act 2008;

Children Act 2004;

Childcare Act 2016;

Data Protection Act 2018 and General Data Protection Regulation (GDPR); and

Equality Act 2021.

4.2 This policy has regard to the following guidance and advice:

Sharing nudes and semi-nudes Advice for Education Settings working with children and young people;

Responding to incidents and safeguarding children and young people (UK Council for Internet Safety December 2021);

Keeping Children Safe in Education (DfE, September 2023);

Preventing and tackling bullying (DfE, July 2017);

The Prevent Duty Departmental advice for schools and childcare providers (Department for Education June 2015) *and*

Searching, screening and confiscation: advice for schools (DfE, July 2022).

4.3 The following School policies, procedures and resource materials are relevant to this policy:

Acceptable Use Policy for pupils;

Staff IT Acceptable Use Agreement;

Safeguarding Policy and procedures;

Anti-Bullying Policy;

Staff Code of Conduct and Protected Disclosure (whistleblowing) policy;

Data Protection Policy for staff;

Remote Learning Policy.

5. Publication and availability

5.1 This policy is published on the School website and is available internally on the School's Policy Drive.

5.2 This policy is available in hard copy on request.

5.3 A copy of the policy is available for inspection from the School office during the School day.

5.4 This policy can be made available in large print or other accessible format if required.

6. Definitions

6.1 In considering the scope of the The Belvedere Preparatory School's online safety strategy, the School will take a wide and functional approach to considering what falls within the meaning of technology, networks and devices used for viewing or exchanging information (collectively referred to in this policy as technology*).*

7. **Responsibility statement and allocation of tasks**

7.1 To ensure the online safeguarding of members of our School community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within The Belvedere Preparatory School.

7.2 **Headteacher and Senior Leaders**

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The Headteacher and Senior Leaders 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
- The Headteacher and Senior Leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The Headteacher and Senior Leaders will work with the Management Board, the Designated Safeguarding Lead (DSL) and IT service provider (Abyss) in all aspects of filtering and monitoring.

7.3 The Proprietor and Management Board

The Management Board is required to ensure that all those with leadership and management responsibilities at the School actively promote the well-being of pupils. The adoption of this policy is part of the Management board's response to this duty.

- The Management Board is responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".
- This review will be carried out by The Management Board whose members will receive regular information about online safety incidents and monitoring reports.
- The Management Board will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

7.4 Online Safety Board Lead

A member of the governing body will take on the role of Online Safety Board Member to include:

- regular meetings with the Designated Safeguarding Lead / Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) as per the DfE Filtering and Monitoring Standards
- reporting to The Management Board
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

7.5 Designated Safeguarding Lead (DSL)

The DSL will:

- hold the lead responsibility for online safety, within their safeguarding role
- receive relevant and regularly updated training in online safety to enable an understanding of the 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
- meet termly with the Online Safety Board Member to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and to ensure that annual (at least) filtering and monitoring checks are carried out
- attend relevant Management Board meetings
- report regularly to the Headteacher and Senior Leadership Team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).
-

7.6 Online Safety Lead

The Online Safety Lead will:

- lead the Online Safety Group
- work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
- receive reports of online safety issues, being aware of the potential for serious child protection concerns, and ensure that these are logged to inform future online safety developments
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness-raising across the school and beyond
- liaise with Curriculum Leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to report immediately those incidents
- provide (or identify sources of) training and advice for staff/ Management Board/ Parents/Carers and learners
- liaise with (school/local authority/MAT/external provider), and support staff (as relevant)
- receive regularly updated training to allow an understanding of how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education: content, contact, conduct and commerce.

7.7 Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme: ProjectEVOLVE . This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

7.8 Teaching and Support Staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to *a member of the Safeguarding Team* for investigation or action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers are 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 activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned learners are 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 lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies.
- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of

7.9 IT Provider

7.9.1 It is the responsibility of the school to ensure that the provider carries out all the online safety measures that the school's obligations and responsibilities require. It is also important that the provider follows and implements school Online Safety Policy and procedures.

7.9.2 The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority / MAT or other relevant body
- there is clear, safe, and managed control of user access to networks and devices
- keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Designated Safeguarding team for investigation and action.

7.10 Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy

- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- 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 related to their membership of the school.

7.11 Parents and Carers

7.11.1 The school will take every opportunity to help parents and carers understand these issues through

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the Learners' Acceptable Use Agreement
- publishing information about appropriate use of social media relating to posts concerning The Belvedere Preparatory School
- seeking their permissions concerning digital images, cloud services
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

7.11.2 Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- the safe and responsible use of their children's personal devices in the school (where this is allowed)

7.12 Community Users

7.12.1 The school encourages the engagement of agencies/members of the community who can provide valuable contributions to the online safety provision and actively seeks to share its knowledge and good practice with other schools and the community.

7.12.2 Community users who access school systems/website/learning platform as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

8. Access to the School's Technology

8.1 The School provides internet, intranet access and an email system to pupils and staff as well as other technology.

8.2 Pupils and staff must comply with the respective Acceptable Use Agreements when using School technology.

8.3 Access by children is monitored by an adult at all times and all such use is monitored teachers and by our IT Provider.

8.4 Pupils and staff require individual user names and passwords to access the Belvedere Preparatory School's internet, intranet (and social media sites where appropriate) and email system which must not be disclosed to any other person.

8.5 Any pupil or member of staff who has a problem with their user names or passwords must report it to the Online Safety Lead immediately.

8.6 No laptop or other mobile electronic device may be connected to the School network without the consent of the Headteacher or Online Safety Lead.

8.7 The use of any device connected to the School's network will be logged and monitored by the Aabyss (including remote working and bring your own device to work).

8.8 The School has a separate Wi-Fi connection available for use by visitors to The Belvedere Preparatory School. A password, which is changed on a regular basis, must be obtained from the Online Safety Lead in order to use it. Use of this service will be logged and monitored by the Online Safety Lead.

9. Procedures for Dealing with Incidents of Misuse

9.1.1 The school will make a flowchart available to staff to support the decision-making process for dealing with online safety incidents.

9.1.2 Staff, pupils and parents are required to report incidents of misuse or suspected misuse to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures.

9.2 Misuse by pupils

9.2.1 Anyone who has any concern about the misuse of technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the anti-bullying policy where there is an allegation of cyberbullying.

9.2.2 Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding Policy and procedures).

9.3 Misuse by staff

9.3.1 Anyone who has any concern about the misuse of technology by staff should report it in accordance with the School's Protected Disclosure (whistleblowing) Policy so that it can be dealt with in accordance with the staff disciplinary procedures.

9.3.2 If anyone has a safeguarding-related concern relating to staff misuse of technology, they should be report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding Policy and procedures.

9.4 Misuse by other users

9.4.1 Anyone who has a concern about the misuse of technology by any other user should report it immediately to the Online Safety Lead or the Designated Safeguarding Lead.

9.4.2 The Belvedere Preparatory School reserves the right to withdraw access to the School's network from any user at any time and to report suspected illegal activity to the police.

9.4.3 If the School considers that any person is vulnerable to radicalisation the school will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

10. Education

10.1 The safe use of technology is integral to the School's Curriculum. Pupils are educated in an age-appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices:

- learner need and progress are addressed through effective planning and assessment
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

10.2 Technology is included in the educational programmes followed in the EYFS in the following ways:

- children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
- children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

10.3 The safe use of technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of PHSe lessons, assemblies and makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week teaching pupils:

- about the risks associated with using the technology and how to protect themselves and their peers from potential risks;
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour;
- and how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

10.4 The safe use of technology aspects of the curriculum are reviewed on a regular basis to ensure their relevance.

10.5 The School's Acceptable Use Agreement for pupils sets out the School rules about the use technology including internet, email, social media and mobile electronic devices, helping pupils to protect themselves and others when using technology. Pupils are reminded of the importance of this policy or, for younger children, the principles of the policy, on a regular basis.

11. Risk assessment

11.1 Where a concern about a pupil's welfare is identified, the risks to that pupil's welfare will be assessed and appropriate action will be taken to reduce the risks identified by the DSL.

11.2 The format of risk assessment may vary and may be included as part of the School's overall response to a welfare issue, including the use of individual pupil welfare plans (such as behaviour, healthcare and education plans, as appropriate).

11.3 Regardless of the form used, the School's approach to promoting pupil welfare will be systematic and pupil focused.

11.3 The Headteacher will have overall responsibility for ensuring that matters which affect pupil welfare are adequately risk assessed and for ensuring that the relevant findings are implemented, monitored and evaluated.

12. Record keeping

12.1 All records created in accordance with this policy are managed in accordance with the School's policies that apply to the retention and destruction of records.

12.2 All serious incidents involving the use of technology will be logged centrally in the technology incident log by the DSL and Online Safety lead.

12.3 The records created in accordance with this policy may contain personal data. The Belvedere Preparatory School has a number of privacy notices which explain how the School will use personal data about pupils and parents. The privacy notices are published on the School's website.

12.4 In addition, staff must ensure that they follow the School's data protection policies and procedures when handling personal data created in connection with this policy. This includes the School's Data Protection Policy and Information Security policies.

13. Filtering and Monitoring

13.1.1 The school filtering and monitoring provision is agreed by the SLT, The Management Board and Abyss and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

13.1.2 Day to day management of filtering and monitoring systems requires the specialist knowledge of both the Safeguarding Team and IT provider to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT Service Provider will have technical responsibility.

13.1.3 The filtering and monitoring provision is reviewed (at least annually) by the Senior Leadership team, the Designated Safeguarding Lead and Board Member with the involvement of the IT Service Provider (Abyss).

13.1.4 Checks on the filtering and monitoring system are carried out by the Online safety lead and IT Service Provider, the Designated Safeguarding Lead, in particular when a safeguarding risk is identified, there is a change in working practice, e.g. remote access or BYOD or new technology is introduced using SWGfL Test Filtering.

13.2 Filtering

13.2.1 The Belvedere Preparatory School manages access to content across its systems for all users and on all devices using the School's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

13.2.2 Illegal content (e.g., child sexual abuse images) is filtered by the School's IT provider (Abyss) by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office.

13.2.3 Requests and approvals for filtering changes are logged and regularly reviewed by the SLT and breaches of the filtering policy are acted upon by the Designated Safeguarding Lead.

13.2.3 Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

13.2.4 If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

13.3 Monitoring

13.1 The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

13.2 The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed and breaches are reported to senior leader

14. Mobile Technologies

14.1 Pupils are not allowed to bring mobile phones in. If a pupil requires a mobile phone to be brought to school for any reason, this must be agreed beforehand by the Headteacher and stored during school time in the school office.

14.2 Staff are not be allowed to use mobile phones whilst working with the children, unless they have permission from the Head Teacher. Examples could include: educational trips off site, residential visits, or authorised photographs during whole school events.

14.3 All staff who work directly with children should leave their mobile phones on silent and out of sight of children in a safe and secure location, e.g. a lockable cupboard.

14.4 Staff should only use their mobile phones in private staff areas during school hours.

14.5 If a call is made to a parent, or to organisations on behalf of Belvedere Preparatory School, a school phone should be used.

14.6 If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

14.6 Volunteers, contractors, and visitors should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or

buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.

14.7 Parents are asked to leave their phones in their pockets and turned off at all times when they are on site. When at school events, please refer to the Digital and Video Images section of this document (16.4).

15. Social Media

15.1 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- Acceptable Use Agreements
- clear reporting guidance, including responsibilities, procedures, and sanctions

15.2 School staff should ensure that:

- no reference should be made in social media to learners, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community
- personal opinions should not be attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

15.3 When official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- a code of behaviour for users of the accounts
- systems for reporting and dealing with abuse and misuse
- understanding of how incidents may be dealt with under school disciplinary procedures.

15.4 Personal Use

15.4.1 Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

15.4.2 Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

15.4.3 School permits reasonable and appropriate access to personal social media sites during school hours.

15.4.4 Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

15.5 Monitoring of public social media

15.5.1 As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.

15.5.2 The Belvedere Preparatory School will respond to social media comments made by others according to a defined policy or process.

15.5.3 When parents/carers express concerns about the school on social media we will encourage them to make direct contact with the school, in private, to resolve the matter.

15.5.4 Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

16. Digital and Video Images

16.1 The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
Guidance can be found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education

16.2 When using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images:

16.3 Staff and volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes unless authorised by the Headteacher.

16.4 Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.
guidance from the Information Commissioner's Office

16.5 Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.

16.6 Learners must not take, use, share, publish or distribute images of others without their permission.

16.8 Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy.

16.9 Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.

16.10 Written permission from parents or carers will be obtained before photographs of learners are taken for use in school or published on the school website/social media. Permission is not required for images taken solely for internal purposes.

16.11 Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.

16.12 learners' work can only be published with the permission of the learner and parents/carers.

17. Online publishing

17.1 The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- *ParentApps:* a connect platform and mobile app

17.2 The school website is hosted by ParentApps. The school ensures that online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

17.3 Where learner work, images or videos are published, their identities are protected, and full names are not published.

18. Data Protection

18.1 The Belvedere Preparatory School has a Data Protection Policy in place and personal data will be recorded, processed, transferred, and made available according to the current data protection legislation.