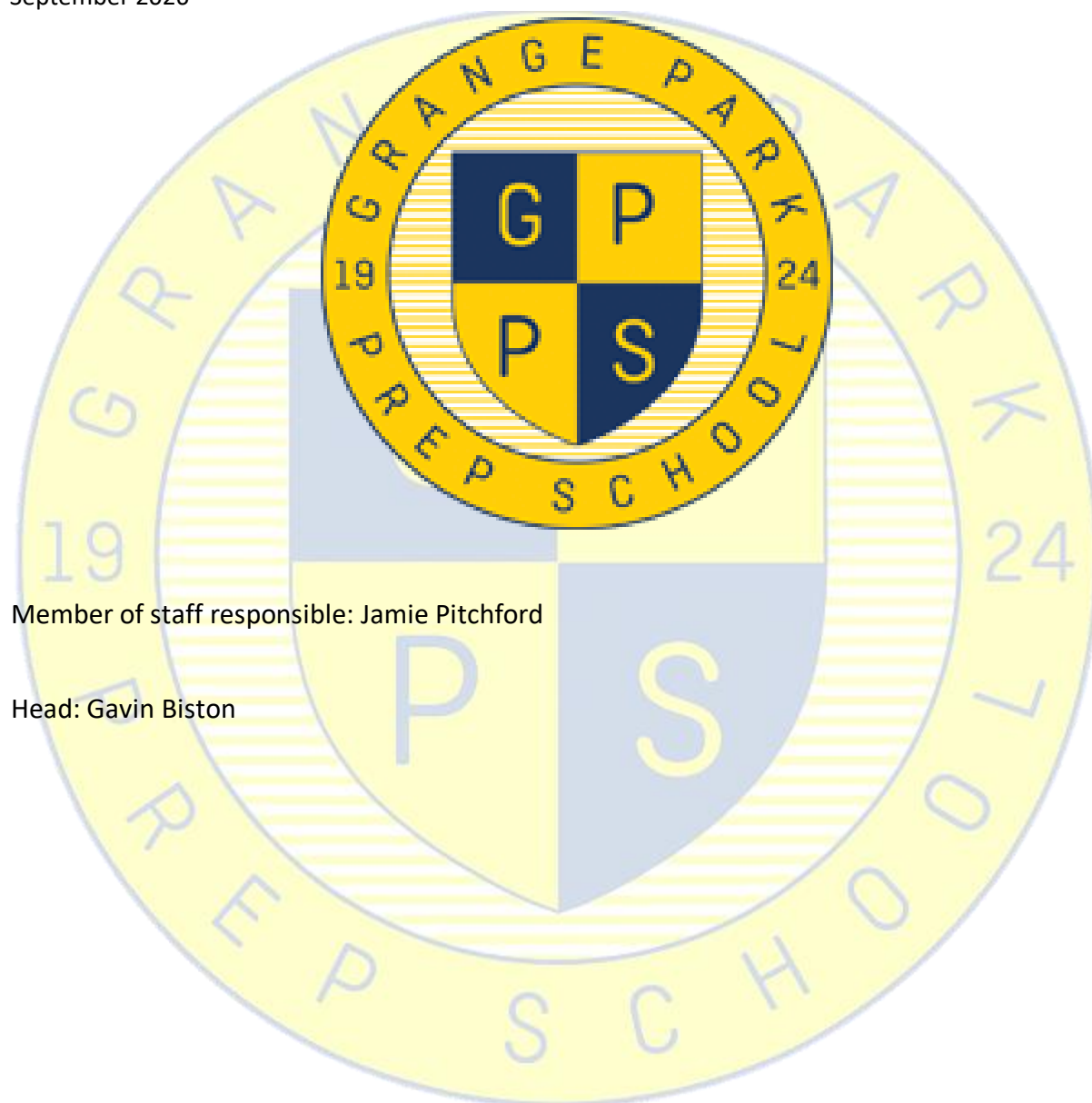


Online Safety Policy

Grange Park Prep School

September 2026



Member of staff responsible: Jamie Pitchford

Head: Gavin Biston

Contents

1.	Introduction and Principles	3
2.	Specific Objectives	3
3.	Areas of Concern	4
4.	Who this Policy is Intended to Cover, and When?	4
5.	Roles and Responsibilities	5
6.	Staff Training	6
7.	Online Safety in the Curriculum and School Community	6
8.	Misuse: Statement of Policy	8
9.	Permitted use of School and Personal Devices	8
10.	Use of Email and other E-Communication	9
11.	Charter for Safe Use of the Internet and Electronic Devices at School	10
12.	Data Storage	11
13.	Password Security	12
14.	Digital Videos and Images	12
15.	Complaints	13
16.	Version Control	13

1. Introduction and Principles

- 1.1. Technology has transformed the process of teaching and learning inside schools. It is a crucial component of every academic subject and is also taught as a subject in its own right.
- 1.2. All of the school's classrooms are equipped with interactive projectors/apple TV and computers.
- 1.3. All our pupils are taught how to research on the internet and to evaluate sources.
- 1.4. They are educated in the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution.
- 1.5. Technology also plays an enormously important part in the lives of all young people outside schools. Sophisticated games consoles, like Xbox, Playstation, Wiis and Nintendo DS, together with internet enabled mobile phones and smartphones provide unlimited access to the internet, to SMS messages, to blogging (web logging), to social media websites (like Twitter), to Skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms and other social networking sites (such as Facebook), and video sharing sites (such as YouTube). This communications revolution gives young people unrivalled opportunities. It also brings risks.
- 1.6. The School takes every step necessary to ensure that all the pupils in its care are safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people.
- 1.7. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

2. Specific Objectives

- 2.1. To set out within the field of technology the areas of concern and action on the part of the School.
- 2.2. To indicate who is affected by this policy and when.
- 2.3. To set out the roles and responsibilities of the School and its staff; and of parents or guardians
- 2.4. To emphasise the importance of staff awareness and training
- 2.5. To identify how the School emphasises the importance of the curriculum in making sure that there is a full understanding of the issues and of how the whole community can be involved in ensuring safety
- 2.6. To indicate our policies on personal devices of staff and children
- 2.7. To indicate our policies on the use of the internet, emails and texts
- 2.8. To set out how we teach staff and pupils to ensure their own safety and that of others by using password security, and ensuring safe data storage and appropriate use of images

- 2.9. To ensure that children are safe from terrorist and extremist material that promote radicalisation when accessing the internet in school, by establishing appropriate levels of filtering and monitoring.
- 2.10. To indicate how a member of the School community (pupil, parent or staff member) can raise a concern/complaint in the event of dissatisfaction arising out of a process or event.

3. Legislative and Regulatory Framework

This policy has regard to the statutory and regulatory framework applicable to an independent school in England, including:

- **Keeping Children Safe in Education 2026 (KCSIE 2026);**
- the **Education (Independent School Standards) Regulations 2014;**
- current DfE guidance on filtering and monitoring;
- current DfE guidance on data protection in schools;
- the **Data Protection Act 2018** and UK GDPR as applicable;
- the **Data (Use and Access) Act 2025**, where applicable;
- the **Counter-Terrorism and Security Act 2015** and Prevent duty guidance;
- the **Equality Act 2010;**
- relevant criminal law concerning communications, images, exploitation, harassment, abuse and cybercrime;
- relevant guidance concerning children and young people's online safety.

The School will also have regard to relevant DfE guidance concerning online safety, mobile phones, remote education and the teaching of online safety.

4. Areas of Concern

- 4.1. New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used both in and outside of School may include:
- Websites;
 - Email and instant messaging;
 - Blogs;
 - Music / video downloads;
 - Text messaging and picture messaging;
 - Video calls;
 - Online communities via games consoles; and
 - Mobile internet devices such as smart phones and tablets.

5. Who this Policy is Intended to Cover, and When?

- 5.1. This policy is implemented to protect the interests and safety of the whole School community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. Whilst exciting and beneficial, both inside and outside

of the context of education, many online resources are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

- 5.2. We understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.
- 5.3. This policy covers both fixed and mobile internet devices provided by the School (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices which might be owned by pupils and staff and brought onto School premises (personal laptops, tablets, smart phones, etc.).
- 5.4. It applies to online activity:
- on School premises;
 - on School-owned devices;
 - using School accounts;
 - using the School network;
 - using School-provided platforms and services;
 - during School trips and activities;
 - during remote education;
- 5.5 When pupils are using School-managed devices away from School; and where activity outside School has a safeguarding or welfare impact on pupils or the School community.
- 5.6 The School recognises that it cannot control all online activity undertaken by pupils outside School. However, where an online incident has an impact on a pupil's welfare, safety, education or the wider School community, the School may need to respond under its safeguarding, behaviour or anti-bullying procedures.

6. Roles and Responsibilities

6.1. Staff

- 6.1.1. All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following School online safety procedures.
- 6.1.2. When children use School computers, staffs make sure children are fully aware of the agreement they are making to follow the School's IT guidelines.
- 6.1.3. To report any concerns about safety to the DSL (Jamie Pitchford) or member of the safeguarding team.
- 6.1.4. To record any concerns on MyConcern
- 6.1.5. To listen to children or adult concerns or worries when raised regarding Online issues.
- 6.1.6. Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise.

6.2. Designated Safeguarding Lead (DSL)

- 6.2.1. The School recognises that online safety is a safeguarding issue. The Designated Safeguarding Lead (DSL) Jamie Pitchford and the Deputy DSLs Gavin Biston and

Becky Collett and EYFS DSL Sam Madden have responsibility for ensuring this policy is upheld by all members of the School community.

- 6.2.2. To keep up to date on current online safety issues and guidance issued by organisations such as the CEOP (Child Exploitation and Online Protection) a national Police Agency, whose hyperlink is: <http://ceop.police.uk/>, Childnet, International and the Local Safeguarding Children Board (LSCB) and NSPCC.
- 6.2.3. To check and monitor Smoothwall and other filter and monitoring devices.
- 6.2.4. To ensure staff are aware of their responsibilities.
- 6.2.5. To ensure the policy is up to date.
- 6.2.6. To promote a culture of talking and learning about e-safety issues.
- 6.3. Parents
 - 6.3.1. The School believes that it is essential for parents to be fully involved with promoting online safety both in and outside of School.
 - 6.3.2. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

7. Staff Training

- 7.1. All new teaching staff receive information on the School's suite of Safeguarding policies as part of their induction, including this policy, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety.
- 7.2. All teaching staff receive regular updates and training about online safety issues that can take place during INSET days or staff meetings.
- 7.3. All specialist staff or staff supporting temporary cover will be referred to a member of the safeguarding team and will refer all concerns that arise to them.

8. Online Safety in the Curriculum and School Community

- 8.1. IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.
- 8.2. The School provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside School will also be carried out via PSHE, as well as informally when opportunities arise.
- 8.3. At age-appropriate levels, pupils are taught to look after their own online safety. Pupils are informally taught about recognising online exploitation of any kind and of their duty to report any such instances which they, or their peers, come across.
- 8.4. Pupils can report concerns to the DSL and any other member of staff at the School.
- 8.5. Children, in KS2, are asked to sign the school's Acceptable Use Policy, this is also shared with parents, this is done at the start of the academic year.
- 8.6. Pupils are taught about respecting other people's information and images (etc.) through PSHCE sessions.
- 8.7. Pupils should be aware of the impact of cyber-bullying (see also the School's Anti-bullying Policy) and the risks posed by adults or young people, who use the internet

and social media to bully, groom, abuse or radicalise other people. Pupils should know how to seek help if they are affected by these issues. Pupils should approach the DSL as well as parents/guardians, peers and other School staff for advice or help if they experience problems when using the internet and related technologies.

8.8. The School utilises Smoothwall to provide a web filtering service.

9. The Four Areas of Online Risk

9.1 The School recognises the four broad categories of online risk:

Content

Children may be exposed to:

- pornography;
- violence and graphic content;
- self-harm and suicide content;
- eating-disorder content;
- extremist and terrorist material;
- hate and discriminatory content;
- misinformation and disinformation;
- age-inappropriate material;
- illegal material;
- harmful challenges;
- harmful or abusive AI-generated content.

Contact

Children may be contacted by:

- strangers;
- individuals pretending to be someone else;
- adults seeking to groom or exploit children;
- individuals seeking sexual contact;
- individuals seeking to radicalise or manipulate children;
- other users seeking to bully, threaten, intimidate or exploit them.

Conduct

Online conduct may include:

- cyberbullying;
- harassment;
- sexual harassment;
- sexual violence;
- sharing intimate images;
- threats to share intimate images;
- impersonation;
- exclusion;

- abuse through group chats;
- livestreaming;
- recording others without consent;
- online gaming abuse;
- harmful online communities;
- discriminatory or hateful behaviour.

Commerce

Children may be exposed to:

- scams;
- phishing;
- fraud;
- financial exploitation;
- gambling;
- inappropriate advertising;
- in-app purchases;
- deceptive online marketing;
- manipulation by influencers or online services.

In order for the school to mitigate the above it will:

- ensure that online safety forms part of the School's safeguarding arrangements;
- ensure appropriate filtering and monitoring systems are in place;
- receive assurance that filtering and monitoring are effective through a process of checking;
- ensure that online safety risks are reviewed;
- ensure that sufficient resources are available;
- ensure that relevant policies are reviewed;

10. Misuse: Statement of Policy

- 10.1. The school will not tolerate the accessing of inappropriate or illegal material and will always report illegal activity to the police and also the LSCB if appropriate.
- 10.2. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP) in addition to the LSCB.
- 10.3. The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-Bullying policy and Behaviour policy.

11. Permitted use of School and Personal Devices

11.1. Staff

- 11.1.1. School devices are assigned to a member of staff as part of their role, these must have a password or device lock so that unauthorised people cannot access the content.

- 11.1.2. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access.
- 11.1.3. Staff are permitted to bring in personal devices for their own use but are not allowed to have their phone switched on during the working day, unless agreed with SLT.
- 11.1.4. They may use their mobile telephone only during break-times and lunchtimes, in designated staff areas.
- 11.1.5. They may use their mobile phone whilst on a school trip to keep in touch with the School.
- 11.1.6. Personal telephone numbers may not be shared with pupils or parents and under no circumstances may staff contact a pupil or parent using a personal telephone number.
- 11.2. Pupils
 - 11.2.1. Mobile technologies available for pupil use [including laptops, tablets, etc.] are stored in a cupboard or desk, with access only available via permission from an adult supervising the children.
 - 11.2.2. No personal devices belonging to pupils are to be used during lessons at School.
 - 11.2.3. If pupils bring in mobile phones (e.g. for safety purposes if they walk to and from School alone), they must be handed in to the Administrator's office at the start of the day and collected as they leave School.

12. Use of Email and other E-Communication

- 12.1. Staff may not access any social networking or personal email, or websites which are unconnected with School work or business, either from School devices or whilst in front of pupils. Such access may only be made from their own personal devices whilst in staff-only areas of School.
- 12.2. There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure.
- 12.3. Staff should be aware that email communications may be monitored.
- 12.4. Staff must immediately report to the DSL or Headteacher the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- 12.5. Any online communications will neither knowingly or recklessly:
 - 12.5.1. place a child or young person at risk of harm;
 - 12.5.2. bring the School into disrepute;
 - 12.5.3. breach confidentiality;
 - 12.5.4. breach copyright;
 - 12.5.5. breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

- 12.5.6. making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
- 12.5.7. using social media to bully another individual; or
- 12.5.8. posting links or material which is discriminatory or offensive.
- 12.6. Any digital communication between staff and pupils or parents is expected to be professional in tone and content. Under no circumstances may staff contact a pupil or parent using any personal email address.

13. Charter for Safe Use of the Internet and Electronic Devices at School

- 13.1. Online safety is a whole school responsibility and the staff have adopted a charter with pupils for the safe use of the internet inside the school with the following elements:
- 13.2. Cyberbullying
 - 13.2.1. Cyberbullying, defined as bullying through the use of electronic devices, is a particularly pernicious form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The school's anti-bullying policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.
 - 13.2.2. Proper supervision of pupils plays an important part in creating a safe ICT environment at school but everyone also learns how to stay safe outside the school.
 - 13.2.3. The School values all of its pupils equally. It is part of the ethos of the school to promote considerate behaviour and to value diversity.
 - 13.2.4. Bullying and harassment in any form, including being targeted or influenced to participate in radicalism or extremism, should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.
- 13.3. Treating Others with Respect
 - 13.3.1. The school expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. They should always follow the school's Behaviour Policy (copies of which are sent to parents).
 - 13.3.2. The school expects a degree of formality in communications between staff and pupils. They should not communicate with each other by text or mobile phones.
 - 13.3.3. Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is set out on the school website. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
 - 13.3.4. All pupils are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the staff.

- 13.3.5. The use of mobile phones within school hours is not allowed in school premises. Pupils who need to have access to a mobile phone out of school hours are instructed to deliver their mobile phone to the School Administrator at the start of the school day and to collect it as they leave school. The use of this mobile phone will not be allowed on school premises, or otherwise until such time as the pupil and mobile have been handed over to their parents' or a designated responsible adult.
- 13.4. Keeping the School Network Safe
 - 13.4.1. The school adheres to best practice regarding e-teaching and the internet
 - 13.4.2. Certain sites are blocked by the school's filtering system and the School is able to monitor pupils' use of the network.
 - 13.4.3. The IT department monitors email traffic and blocks SPAM and certain attachments.
 - 13.4.4. The school has anti-virus protection on its network which is administered by the school's IT support.
 - 13.4.5. Any pupil who wishes to connect a removable device to the school's network is asked to arrange in advance with their class teacher who will ensure the appropriate clearances
- 13.5. There is strong anti-virus and firewall protection on our network and certain websites are automatically blocked by the School's filtering system; in addition, spam emails and certain attachments will be blocked automatically by the email system. If these issues cause problems for School work or research purposes, pupils will speak to their classroom teacher for assistance.
- 13.6. Pupils should immediately report, to their teacher or DSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- 13.7. Pupils must report any accidental access to materials of an inappropriate nature [e.g. if violent or sexual] directly to a teacher who must then inform the DSL, recording this on MyConcern. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the School's Behaviour Policy. Pupils are aware that all internet usage via the School's systems may be monitored.
- 13.8. The School expects all pupils to adhere to this policy for the safe use of the internet.
- 13.9. To ensure that there are no incidents of misuse, or attempted misuse of the internet, personal mobile phones and other electronic devices are not permitted to be used to access the school's ICT facilities.

14. Data Storage

- 14.1. The School takes its compliance with the Data Protection Act 2018 seriously.
- 14.2. Staff and pupils are expected to save all data relating to their work to the School's central server or Google Drive Account.
- 14.3. Staff devices should be encrypted if any data or passwords are stored on them. The School expects all removable media (USB memory sticks, CDs, portable drives) taken outside School or sent by post or courier to be encrypted before sending.

- 14.4. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks but instead stored on an encrypted USB memory stick provided by School.
- 14.5. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the class teacher.

15. Password Security

- 15.1. Pupils and staff have individual School network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security. All pupils and members of staff are encouraged to:
 - 15.1.1. use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers and special characters), which should be changed as a minimum every school year;
 - 15.1.2. not write passwords down; and
 - 15.1.3. not share passwords with other pupils or staff.

16. Digital Videos and Images

- 16.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.
- 16.2. When using digital images, staff 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).
- 16.3. In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at School events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images may not be published on blogs or social networking sites (etc.), nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- 16.4. Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on School equipment: personal equipment should not be used for such purposes.
- 16.5. Care is 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. Pupils may not take, use, share, publish or distribute images of others without their permission.
- 16.6. Written permission from parents will be obtained before photographs of pupils are published on the School website or elsewhere.

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

17. Complaints

- 17.1. As with all issues of safety at the School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it.
- 17.2. Complaints should be addressed to the class teacher in the first instance, who will undertake an immediate investigation and liaise with SLT and any members of staff or pupils involved.
- 17.3. Please see the Complaints Policy for further information.
- 17.4. Incidents of or concerns around online safety will be recorded using MyConcern form and reported to the School's DSL in accordance with the School's Child Protection Policy.

18. Version Control

Date of adoption of this policy	January 2017
Date of last review of this policy	March 2026
Date for next review of this policy	March 2027
Policy owner	Mr Jamie Pitchford
Policy owner	Mr Gavin Biston