BRACKENFIELD SCHOOL

E-SAFETY & ONLINE SAFETY POLICY

Author	Jean-Claude Olesqui & Sarah Haslop	Head of IT DSL
Approved by	Joe Masterson	Headmaster
	John Forsyth	Chairman of the Forfar Education Group Governance Board for Harrogate Preparatory School Ltd, trading as Brackenfield School
Next review	April 2027	

INTRODUCTION

What is the E-safety and online safety policy?
Online safety is an integral part of safeguarding. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' (KCSIE latest version) and other statutory documents; it is designed to sit alongside the school's Child Protection and Safeguarding Policy. This policy also reflects guidance from Working Together to Safeguard Children and DfE filtering and monitoring standards.

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

This policy should be read in conjunction with:

- Safeguarding & Child Protection Policy
- Prevent Duty Policy
- Anti-Bullying Policy
- Behaviour Policy
- KCSiE (latest version)
- Remote Learning Policy

AIMS

This policy aims to:

- Set out expectations for all Brackenfield staff and pupils' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns.
- Respond to emerging online safety risks (e.g. harmful online trends, misinformation, AI-generated content) through regular staff updates and curriculum adaptation

ROLES & RESPONSIBILITIES

Headmaster's Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the Designated Safeguarding Lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported.
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding.

- Liaise with the Designated Safeguarding Lead and online safety coordinator on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DSL, Chairman of the Governing Body and senior leadership team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always a priority and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure all remote learning policies are kept up to date
- Ensure the school website meets statutory requirements.

Designated safeguard lead (DSL), and IT lead

The DSL and IT lead at Brackenfield School will collaboratively lead responsibility for Child Protection and Safeguarding (including online safety).
The IT lead will work alongside the DSL to ensure an effective approach within the school.

Key Responsibilities;

- Liaise with the local authority and work with other agencies in line with Working Together to Safeguard Children
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the Headmaster and senior leadership team to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the headteacher
- Receive regular updates in online safety issues and legislation, be aware of local and school trends
- Ensure that online safety education is embedded across the curriculum and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents
- Liaise with school technical, pastoral, and support staff as appropriate

- Communicate regularly with the senior leadership team and the Designated Safeguarding Lead to discuss current issues (anonymised), review incident logs and filtering/change control logs and discuss filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Oversee and discuss 'appropriate filtering and monitoring' with the head and ensure staff are aware
- Ensure the 2021 Department for Education guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying
- Facilitate training and advice for all staff
- All staff must read KCSIE Part 1 and all those working with children Annex A
- It would also be advisable for all staff to be aware of Annex C (online safety)
- Cascade knowledge of risks and opportunities throughout the organisation
- Keep all remote learning policies up to date
- Ensure that filtering and monitoring systems are effective, regularly reviewed and in line with DfE guidance. Safeguarding alerts generated by monitoring systems will be reviewed daily, with concerns reviewed and actioned in line with safeguarding procedures. The DSL retains overall responsibility for safeguarding responses.

All staff

Key responsibilities:

- Follow the remote learning policy and teacher protocols during any part or full school closure
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and IT lead are
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for Senior management team and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main child protection and safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff code of conduct
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology (devices, the internet, remote learning, new technology such as augmented reality, etc) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites (ask your IT coordinator what appropriate filtering and monitoring policies are in place)

- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, remote learning, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law
- Encourage pupils to follow their acceptable use policy
- Notify the DSL or IT lead of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often most likely to see or overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the IT Leadand have a healthy curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff
- Report any low-level concerns regarding online conduct (their own or others') in line with the staff code of conduct and safeguarding procedures

PSHE & C Lead

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE/ Relationships Education curriculum, complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds.
- Work closely with other staff to ensure an understanding of the issues, approaches and messaging within PSHE and Relationships Education.

IT lead

Key responsibilities:

- As listed in the 'all staff' section
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for IT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Volunteers and contractors

- Read, understand, sign and adhere to the acceptable use policy (AUP)
- Report any concerns, no matter how small, to the DSL/IT lead
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

- Read, understand and adhere to the pupil acceptable use policy, including the remote learning responsible use policy for pupils and review this annually.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies (including remote learning policies) cover actions out of school, including on social media
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/ carers

- Consult with the school if they have any concerns about their children's use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, Proprietor, contractors, pupils or other parents/carers.
- Read, agree and counter sign the Pupil acceptable use policy, when this is shared by the school.

TEACHING & LEARNING

Why Internet and digital communications are important

- The Internet is an essential element in modern life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience and to teach them to use the internet safely.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.
- Filtering appropriate to the age of pupils is provided by Lightspeed web filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Keeping pupils safe online

Teaching of IT and internet skills at Brackenfield, includes ensuring all pupils and staff remain safe when accessing the internet and understand 'What to do.' If a situation occurs when using the internet that upsets, endangers or exposes pupils to inappropriate material in and out of school. These can be categorised into three main risk areas:

- Content: Being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behavior that increases the likelihood of or causes harm.

The school recognises that some pupils, including those with SEND, SEMH needs or those who are looked after, may be more vulnerable to online risks. Additional support and targeted teaching will be provided where appropriate.

Handling online safety concerns and incidents
It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of ICT, PSHE and Citizenship).

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all staff should err on the side of talking to the online-safety coordinator / Designated Safeguarding Lead to contribute to the overall picture or highlight what might not yet be a problem. All online safety concerns will be recorded in the school's safeguarding recording system. Records will be detailed, dated and reviewed by the DSL to identify patterns, links and wider safeguarding concerns.

Non-teaching staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

The school's procedures for dealing with online-safety are mostly detailed in the following policies (primarily in the first key document):

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

Brackenfield school commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact on pupils when they come into school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the DSL on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headmaster in which case the complaint is referred to the Chair of the Governing Body and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law.

INTERNET USE

The School recognises the benefits to using the Internet in an educational environment. The Internet facility is provided for school related activities only. The school monitors the use of the Internet.
The school internet system has a filtering and monitoring system run by Lightspeed, which monitors and filters all website access against preset policies. Any inappropriate material, whether it be

sexual, violent, extremist or illegal in nature will be blocked and the System Administrator alerted, who will in turn alert the school DSL/IT lead as to the inappropriate material being accessed.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Pupils will be taught how to report unpleasant or upsetting Internet content

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective

Authorising Internet access

- All staff must read and sign the Staff Code of Conduct before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems
- All junior pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access
- Any person not directly employed by the school will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site
- Children must only access the internet for research via a laptop through their personal login details. iPad/Safari must not be used for researching via the internet.

GOOD PRACTISE FOR STAFF, PUPILS AND PARENTS

Staff Personal Safety

It is vitally important that staff are careful about content that they search out or download. Every time you view a page on the internet, it is possible to trace your visit back to the school computer. This means that it is possible to tell if the school computer was being used to look at inappropriate web pages.

Staff need to ensure that films or other material shown to children are age-appropriate.

Staff must be aware of their responsibilities to the school when using social networking sites such as Facebook. Our staff code of conduct and confidentiality policy must be adhered to at all times, even outside of working hours. It is important to maintain your status as a professional teacher.

Disciplinary action could result if the school is brought into disrepute.

- Staff must not post anything on any online site that could be construed to have an adverse impact on the school's reputation
- Staff must not post photos related to the school on any internet site including pupils, parents, staff or the school branding (uniform)

- Staff must not form online friendships with pupils and parents
- Staff must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school
- Staff will be required to attend an annual internet safety course and ensure that they pass this information on to the children in their care. This can be either online or delivered by the online-safety co-ordinator, Mr Olesqui within staff meetings.
- Staff should use their school email account for all school-related communications
- Staff members should refer to the Acceptable Use Policy for more detailed information

Pupil Personal safety

- The school will ensure online safety and good practise is taught to all year groups, year round
- Pupils must not play with or remove any cables etc that are attached to a school computer
- Pupils will be taught how to stay safe when working online at school and at home
- Pupils must not post anything on to social networking sites that would offend any other member of staff, pupil or parent using the school
- Pupils must not post anything on any online site that can be constructed to have an adverse impact on the school's reputation
- Pupils must not post photos or video related to the school on any internet sites including pupils, staff, parents or the school branding (uniform)
- Pupils should never reveal their full name, any address or contact details, any school or network user ID or password online, even if communicating with known acquaintances
- Pupils should be aware that the potential exists for predators to remain entirely anonymous and easily pose as someone else.
- Pupils should employ a healthy mistrust of anyone that they "meet" online unless their identity can be verified.
- The use of chat rooms and social networking sites are not permitted in school.
- Do not arrange to meet anyone you have met on the internet - people are not always who they say they are.

Parents

- Parents need to be aware that parental control software is often available via their ISP so that they can manage and control their child's computer and internet activity. Mobile phone operators also offer free parental control software services to limit the kind of content your children can access through the mobile network.
- Parents need to be aware that the parental control software doesn't replace the need for supervision and education when working on the internet.
- Computers for children should be used in a shared space where parents can see the screen.
- Parents should take an interest in their children's internet use and discuss various issues pertaining to the internet.
- Parents should be aware of various age limits on games and social networking sites. These are there for a reason.
- Parents should discuss the care needed when their children meet online "friends". (Only talk to people they know). Parents should remind their children not to give out any personal details nor details of family and friends, even to people they know.

- Parents should encourage their children to tell them if anything online makes them feel uncomfortable.
- Parents should make their child aware of the dangers of meeting someone they have only met online.
- Parents should be aware that they are in control and that they have every right to check on their children's online activities as well as their mobile usage.
- Parents should encourage offline activities. Socialising with friends and taking part in physical activities is really important.
- A link to several resources relating to advice on how parents can support their child to be safe using IT can be found on the school website under the section School Life/E-Safety.

You can find out more about how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to children about e-safety at;

The UK Safer Internet Centre website

http://www.saferinternet.org.uk

CEOP's Thinkuknow website

http://www.thinkuknow.co.uk

http://www.thinkyouknow.co.uk/parents

Internet Matters

http://www.internetmatters.org

Childnet

http://www.childnet.com/sns

NSPCC

http://www.nspcc.org.uk/onlinesafety

Parent Zone

http://www.parentzone.org.uk

Ask About Games (where families make sense of video games)

http://www.askaboutgames.com

INAPROPRIATE BEHAVIOUR

Bullying of another person will not be tolerated at Brackenfield School

- Lessons concerning cyber bullying to be carried out termly through the computing and PSHE curriculum.
- By cyber bullying, the School is referring to: bullying by email, messages, images, calls or other electronic communication.
- Use of mobile phone cameras to cause distress, fear or humiliation.

- Posting threatening, abusive, defamatory or humiliating material on websites (including social networking sites).
- Hijacking or hacking email accounts.
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms or on instant messaging services.
- The use of Social Media for the use of bullying, grooming, abuse and radicalisation.

Pupils should be aware that cyber bullying is generally criminal in character and that English law does apply. The School will endeavour to resolve all matters using the School's Behaviour Policy without Police involvement, but parents of victims do have the right to seek Police intervention. This will be closely linked to the School's Anti-Bullying Policy and Brackenfield's Safeguarding and Child Protection Policy which can be read separately or in conjunction with this policy.

Concerns as a parent
Before doing anything, take a deep breath and remain calm. There's lots of information and advice on the http://www.thinkyouknow.co.uk site to keep your child safe and access support.

Having a calm and open conversation is one way for you and your child to explore what is happening in an honest and supportive way.

Discuss your concerns with someone you trust, for example a friend, partner or the school.

You can also talk to a professional at the NSPCC helpline on 08001111.

Talking about it will help decide the best action to take to ensure your child is safe.

To make a report
If you are concerned about online grooming or sexual behaviour online you can contact CEOP: http://www.ceop.police.uk or alternatively you can click on the 'Report Abuse' button located at http://www.thinkyouknow.co.uk.

If you stumble across criminal sexual or obscene content on the internet you should report it to the Internet Watch Foundation: http://www.iwf.org.uk.

You can also report directly to your local police force. If you think your child is in immediate danger call 999.

REMOTE LEARNING, COMMUNICATION & ONLINE LEARNING.

The school uses a range of websites to enhance pupils school education, which include pupils to access learning material set by teachers, complete school work online, communicate and if the situation occurs and the school is required to close, access home learning. These websites require a login and all logins are administered by the appropriate administrators (school office, Softegg and ICT co-ordinator) in accordance with the school's GDPR. These sites are accessible online and via direct apps on the school Ipads or laptops. Staff must ensure that all online interactions with pupils are professional, recorded where possible, and take place via approved school platforms only. One-to-one communication should be avoided unless necessary and must be transparent and logged.

The sites that pupils access and have login details are:

- Teams
- Atom

- Spelling framework
- Kodeable
- Code.org

TEAMS

Microsoft Teams is used as an online learning and communication tool and will be the primary resource used if the school is required to close and pupils are required to access learning from home. At other times, pupils are able to access school work and resources set by teachers, online chat with teachers and join video conferencing.

Inline with GDPR and the schools E-safety policy:

- Private online 'chat' is not accessible by pupils with the class teacher, IT lead and school Head having overall access and monitoring of any communication via Teams.
- The communication is limited to open classroom messaging.
- Pupils are not able to create or attend video conferencing unless administered and monitored by school teachers.
- Pupils are required to follow and adhere to the schools acceptable use policy when using Teams within school and outside of school.

EMAIL USE

Personal use

Email is provided for school related purposes only. The school monitors the use of email and disciplinary action may be taken if inappropriate uses of personal emails are discovered.

Status

Email should be treated in the same way as any other form of written communication. Anything that is written in an email is treated in the same way as any form of writing. Pupils and staff should not include anything in an email that is not appropriate to be published generally. Any email message which is abusive, discriminatory on grounds of sex, race, disability, sexual orientation or religious belief, or defamatory is not permitted.

Privacy

All files and emails on the system are property of the School. As such, system administrators and staff have the right to access them if required.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a teacher or parent/guardian if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- The school will consider how e-mail from pupils to external bodies is presented and controlled

System security

Monitoring

The school reserves the right to monitor the use of the network, internet and e-mail systems. If it is discovered that any of the systems are being abused and/or that the terms of this policy are being breached, appropriate disciplinary action will be taken.

Property

Pupils and staff should treat any property belonging to the school with respect and reasonable care and report any faults or breakages to a member of office staff.

Viruses

Pupils and staff should be aware of the potential damage that can be caused by computer viruses. Pupils and staff must not download, install or run any programs or data (including computer games) or open emails from unknown or unidentifiable sources.

System Security

- All computers and laptops are password protected. Staff are required to change their password on a 3 month basis
- Pupils should not attempt to gain unauthorised access to anyone else's user area or to any information which they are not authorised to access
- Do not make deliberate attempts to disrupt or damage the school network, any device attached to it or any data stored on it or transmitted across
- Do not alter school hardware in any way
- Do not knowingly misuse headphones or any external devices e.g. printers, mouse's.
- Do not eat or drink while using the computer
- All users should log out of any device properly as well as ensure the device is shutdown in order to protect user data

Leaving workstations

If a person leaves their workstation for any period of time they should log out of their workstation.

DIGITAL IMAGES AND VIDEOS

The word photography is used in this policy to include traditional photographs and digital images of any kind, still or moving.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used.

Photography and video are familiar features of life, playing a significant role in commerce, entertainment and communication; it is commonplace in our homes and it is an important element of school life.

At Brackenfield we feel it is vital that achievements are recognised and that pupils feel valued, proud and happy. Photography is a useful tool within school and it is employed routinely in many ways, for example; record keeping, displays, special events, teachers' lessons and the children's own work.

On occasions photos are also used for the Press, school website, school facebook page and other promotional purposes, following the strict Consent list which is updated every 12 months.

Children will only be named in photographs that are displayed within the school. We will not provide children's full names for any other purpose unless special parental consent has been received.

We are, however, sensitive to the wishes and rights of parents who may not wish their children to be photographed and who may have concerns about the use of such images.

Taking photos and videos

All parents are asked to give consent for photography of their child by completing a permission slip that is held on file. A register is kept of children who must not be included in press, website or any other photographic image, still or moving.

All reasonable measures will be taken to ensure that no child on the register is photographed or videoed by a visitor to school or while on an educational visit outside school. The exception to this may be photographs taken by parents at events such as sports fixtures and performances.

From time to time we invite the Press into school to share special events and achievements within the local community. We will allow local newspapers to take photographs of children, when appropriate, provided that parental consent has been given.

Some newspapers insist that children's names must be published with their photographs. If not, they may decline to cover school events. Therefore, we will normally give the children's full names (but not addresses) to newspapers only if requested by them. That is why it is important for you to tell us whether you have any objections.

Images taken by school staff

Only the school's cameras or video equipment are to be used by staff when taking photographs. All equipment must be returned to the school office.

The printing of images is always carried out on the school premises. All photographic images held on devices will be deleted at the end of each week.

All images taken must be deemed suitable without putting the child in any compromising positions that could cause embarrassment or distress.

Under no circumstances will a camera be allowed into the bathroom areas unless a member of the Senior Leadership Team (SLT) is present. For example, if staff in the Early Years would like photos of the children washing their hands for hygiene posters a member of the SLT must be present.

Photographs taken as records of events or for educational purposes may be displayed around the school. They are then archived or shredded after use.

Photographs used for evidence in the Early Years Learning Journeys are saved digitally and kept in line with GDPR guidelines. Parents have access to an online platform until the end of their child’s Reception Year.

Photographs are not exchanged with anyone outside school or removed for private use by any employee or volunteer.

Images taken by children
There is no reason why pupils should not be allowed to take photographs so long as anyone photographing respects the privacy of the person being photographed. This is seen as part of the school's code of behaviour.

Infringement of this respect of privacy is akin to bullying and will be dealt with in the same way as any other breach of school discipline.

Pupils are not normally allowed to bring to school or take on trips any electronic devices such as tablets, smartphones, smartwatches, laptop or other computer devices which have the capability to film videos or internet access. Exceptions will be considered for residential trips, when expectations of use are clearly laid out and monitored by trip leader.

Should the school learn about any inappropriateness of image use involving our pupils or staff, we will immediately act and report it as we would for any other child protection issue.

SOCIAL MEDIA

Staff, pupils and parent's social media
Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.

However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and

when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Email is the official electronic communication channel between parents and the school.

Pupils and parents are not allowed* to be 'friends' with or make friend requests** to any staff, volunteer and contractor or otherwise communicate via social media.

Pupils and parents are discouraged from 'following' staff, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public pupil accounts.

* Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the Head and should be declared upon entry of the pupil or staff member to the school).

** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Head (if by a staff member).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school on social media and be careful that their personal opinions might not be attributed to the school, trust or local authority, bringing the school into disrepute.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video and permission is sought before uploading photographs, videos or any other information about other people.

USE OF MOBILE PHONES

Pupils

- Pupils are not permitted to bring mobile phones, smartwatches or personally owned devices into school.
- Pupils in Year 6 who have been given permission by the Head to walk to and from school must sign in their mobile phones at the school office when they arrive in the morning for safe-keeping in a locked location during school hours.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with school policy.

Staff

See staff code of conduct and or Acceptable Use Policy

PUBLISHING AND CONTENT

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.

- The School admin staff will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing photographs, images and work (including EYFS online platforms)

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by ensuring names are not linked with photographs. The school will look to seek to use group photographs rather than full-face photographs of individual children.
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs or images of pupils are published
- Written permission from adults will be obtained before their names, photographs or images of themselves are published
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites during school time and consider how to educate pupils in their safe use e.g. use of passwords, privacy settings
- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location
- Pupils must not place personal photos on any social network space provided in the school learning platform without permission
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites
- Pupils will be advised to seek adult help or to report any offensive or upsetting material

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to Mr J C Olesqui
- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other devices

- Mobile phones tablets (or equivalent technology) and associated cameras will not be used during lessons or formal school time including PPA except as part of an educational activity.
- The sending of abusive, offensive or inappropriate material is forbidden.
- School reserves the right to check any mobile technology used in school at any time
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care will be taken with their use within the school use
- Staff should not share personal telephone numbers with pupils and parents. Staff telephone numbers will only be provided for emergency use out of school hours during residential school trips

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 & GDPR *updated 2021*

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headmaster
- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead and dealt with in accordance with school child protection procedures
- Pupils and parents will be informed of the complaint's procedure
- Pupils and parents will be informed of consequences for pupils misusing the Internet

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on E-safety.

Artificial Intelligence (AI) and Generative Technologies

The school recognises the increasing use of AI and generative technologies (e.g. chatbots and content-generation tools). While these can support learning, they also present risks including inaccurate information, exposure to inappropriate content and data privacy concerns.

- Staff must not input personal or sensitive pupil data into AI tools.
- Pupils will be taught to critically evaluate AI-generated content.
- Use of AI tools in school will be risk assessed prior to use.
- Staff will be supported through training to understand the safeguarding implications of AI.

Name of policy E-Safety & Online Safety Policy	**Policy reviewed/amended date** March 2023 V2 January 2024 V3 September 2024 V4 April 2025 V5 April 2026 V6 May 2026 V7 (minor updates)
Original policy date November 2021	**Current version** V7
Date of new review May 2027	