



OLD BUCKENHAM HALL

A leading co-educational preparatory school for children aged 2-13 years

Old Buckenham Hall School

Online Safety Policy

Advent 2026

Key School Contacts	
Mrs Emma Easedale, DSL, School Nurse	Email: emma.easedale@obh.co.uk Telephone number (term time): 01449 744782 Mobile number (term time): 07776691665 Holiday contact number: Mobile number as above
Online Safety Co-ordinator Mr Andrew Swiney	Email: andrew.swiney@obh.co.uk Telephone (term time): 01449 740252
School Technical Support: John Sibley	Email: john.sibley@obh.co.uk Telephone: 01449 740252
Deputy Designated Safeguarding Leads (DDSL)	
Mr James Large, Headmaster	Email: headmaster@obh.co.uk Telephone (term time): 01449 740252
Mr Graham Drury, Deputy Head Pastoral	Email: graham.drury@obh.co.uk Telephone (term time): 01449 740252
Miss Rebecca Devine - Head of Middle School	Email: rebecca.devine@obh.co.uk Telephone (term time): 01449 740252
Mrs Jessica Ewart, Head of EYFS	Email: jess.ewart@obh.co.uk Telephone: 07776691665
Additional Key Contacts	
Director of IT (Rugby Group) Pieter van der Walt	Email: pdvw@rugbyschool.net
Group Director of Safeguarding Charlotte Marten	Email: cm1@rugbyschool.net
Nominated Safeguarding Governor/Online Safety Governor Flora McLean	Email: fl@rugbyschool.net Telephone number: <u>07790 905811</u>

CONTENTS

1.1 AIMS	4
1.1.2 RISKS AND VULNERABILITIES.....	4
1.2 REGULATORY FRAMEWORK	5
1.3 DEFINITIONS	5
1.4 ROLES AND RESPONSIBILITIES IN RELATION TO ONLINE SAFETY	5
1.4.1 THE GOVERNING BODY	5
1.4.2 HEAD AND THE SENIOR LEADERSHIP TEAM	6
1.4.3 THE DESIGNATED SAFEGUARDING LEAD (DSL)	6
1.4.4 ONLINE SAFETY COORDINATOR.....	6
1.4.5 IT STAFF	6
1.4.6 TEACHING AND SUPPORT STAFF	7
1.4.7 PUPILS.....	7
1.4.8 PARENTS AND CARERS	7
2. SCOPE AND APPLICATION	7
3. 1 FILTERING AND MONITORING.....	8
3.1.1 STAFF	8
3.1.2 PUPILS.....	9
3.2 EDUCATION AND TRAINING.....	9
3.3 USE OF PERSONAL DEVICES	10
3.3.1 STAFF	10
3.4 ONLINE COMMUNICATIONS	12
3.4.1 STAFF	12
3.4.2 PUPILS.....	12
3.6 DATA PROTECTION	13
3.7 PASSWORD SECURITY	14
3.8 SAFE USE OF DIGITAL AND VIDEO IMAGES	14
3.10 MISUSE	15
3.11 COMPLAINTS.....	15
4. POLICY OWNER	15
5. RELATED POLICIES AND GUIDANCE	15
APPENDIX 1	17
SANCTIONS IN RELATION TO THE MISUSE OF IT	17
APPENDIX 2 ONLINE SAFETY TEACHING AT OLD BUCKENHAM HALL SCHOOL	19

1. INTRODUCTION

1.1 AIMS

It is the duty of Old Buckenham Hall School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. Online communications and technology provide opportunities for enhanced learning but also pose great risks to young people. 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 bullying, harassment, grooming, stalking, abuse, misogyny, radicalisation and identity theft.

Technology is continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. However, many information technologies, particularly online resources, are not effectively policed. All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;
- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policies for staff, visitors and pupils, 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.

At Old Buckenham Hall School, 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. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

1.1.2 RISKS AND VULNERABILITIES

Abuse that occurs online should be treated with the same seriousness as abuse that occurs offline in the real world.

The school acknowledges that some pupils are particularly vulnerable to being abused online. These include but are not limited to:

- pupils with a SEND who may find it difficult to distinguish between fact and fiction in online content and may repeat content or behaviours encountered online without understanding the consequences
- pupils whose first language is not English.

Harmful sexual behaviours, sexual harassment, sexual abuse, physical and emotional abuse may all have an online element or be conducted solely online. Abuse may occur solely offline, but staff will be alert to the possibility of abuse may be happening concurrently both offline and online. Similarly, staff will be alert to the possibility that older pupils may be drawn into cybercrime or recruited into a county line through contacts that they have made online.

1.2 REGULATORY FRAMEWORK

This policy has regard to the following guidance and advice:

- *Keeping Children Safe in Education* (September 2026) ("KCSIE")
- *Prevent duty guidance: Guidance for specified authorities in England and Wales December 2023*. Prevent is supplemented by a briefing note:
 - *How social media is used to encourage travel to Syria and Iraq* (July 2015)
- *Relationships Education, Relationships, and Sex Education (RSE) and Health Education* (July 2025).
- *Behaviour in schools* (February 2024)
- *Digital and technology standards in schools and colleges* (August 2026)
- *The National Minimum Standards for boarding schools* (May 2026)
- *Early Years and Foundation Stage Statutory Framework* (July 2026)
- *Advice for Early Years Practitioners on Screen Use* DfE (July 2026)
- *Safeguarding children and protecting professionals in early years settings: online safety considerations* UK Council for Internet Safety (February 2019)

1.3 DEFINITIONS

Head is the Headmaster of Old Buckenham Hall School

Parents includes pupils' parents, carers and guardians.

Pupils includes all children who are registered and attend the school.

Staff includes teaching staff, support staff (operational and administrative staff), trainee teachers, supply staff, governors and volunteers

Visitors includes anyone who is not a pupil, parent or member of staff who comes into the school.

1.4 ROLES AND RESPONSIBILITIES IN RELATION TO ONLINE SAFETY

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in line with the Child Protection and Safeguarding Policy.

1.4.1 THE GOVERNING BODY

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Child Protection and Safeguarding Policy. The Governing Body of the school is responsible (via its Safeguarding Committee) for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the Online Safety Coordinator, DSL and Senior Leadership Team, are adequately trained about online safety;
- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

The Safeguarding Committee of the Governing Body will review the school's progress towards meeting the DfE's Digital and Technology Standards.

1.4.2 HEAD AND THE SENIOR LEADERSHIP TEAM

The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with the Senior Leadership Team, they are responsible for feeding into group decisions relating to procuring appropriate filtering and monitoring systems, ensuring that decisions on what is blocked or allowed and why are documented, reviewing the effectiveness of the filtering and monitoring provisions at least annually, overseeing reports in relation to online safety and ensuring that staff are appropriately trained.

1.4.3 THE DESIGNATED SAFEGUARDING LEAD (DSL)

The DSL takes the lead responsibility for Safeguarding and Child Protection at Old Buckenham Hall School. This includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSL will ensure that this policy is upheld at all times, working with the Head and Senior Leadership Team, the Online Safety Co-ordinator and IT staff (at both local and group level) to achieve this. As such, in line with the Child Protection and Safeguarding policy, the DSL will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSL will work closely with the Online Safety Co-ordinator and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSL will review filtering and monitoring reports and ensure that checks are conducted to ensure that filtering and monitoring is working on all internet enabled devices in all locations across the school as required by KCSIE paragraph 171. The DSL will report to the Group's Director of Safeguarding and the governors' Safeguarding Committee on progress towards meeting the DfE's Digital and Technology Standards.

1.4.4 ONLINE SAFETY COORDINATOR

The DSL has delegated day to day responsibilities relating to online safety to the school's Online Safety Coordinator. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education, ISI, the CEOP (Child Exploitation and Online Protection), Childnet International and the Local Safeguarding Children Procedures. The Online Safety Coordinator will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system with the DSL.

1.4.5 IT STAFF

The school's IT staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and

administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Online Safety Coordinator. In doing this, they work in partnership with the Director of IT.

1.4.6 TEACHING AND SUPPORT STAFF

All staff are required to sign and return the Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it and the school's Acceptable Use Policies in accordance with direction from the DSL and the Head as appropriate.

Staff are responsible for monitoring the use of digital technologies and, mobile devices and cameras in lessons and in other school activities where they are allowed. They may also be responsible for delivering aspects both formal and informal of the online safety curriculum (see Appendix 2).

1.4.7 PUPILS

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy.

1.4.8 PARENTS AND CARERS

Old Buckenham Hall School believes that it is essential for parents to be fully involved with promoting online safety both within and outside school. 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. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

2. SCOPE AND APPLICATION

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, chrome books, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches, digital cameras etc.).

In designing this policy, the school has considered the "4Cs" outlined in KCSIE (content, contact, conduct and commerce) as the key areas of risk. However, the school recognises that some pupils will have unlimited and unrestricted access to the internet via mobile phone networks. This means that some pupils, may use mobile technology to facilitate child-on-child abuse, access inappropriate or harmful content or otherwise misuse mobile technology in the evenings (if they are day pupils) and during the holidays. The improper use of mobile technology by pupils, in or out of school, will be dealt with under the school's Behaviour Policy and/or Child Protection and Safeguarding Policy as is appropriate in the circumstances (See Appendix 1 for detail relating to sanctions).

This policy applies **at all times** including where pupils or staff are away from the school, whether they are on school arranged activities or otherwise, and whether or not the school is open i.e. it applies out of school hours and in the holidays.

3. 1 FILTERING AND MONITORING

Old Buckenham Hall School aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring. The school uses Lightspeed to filter access and monitor online activity.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Coordinator will check at least termly that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. They will ensure that over the course of a year, the requirement (KCSIE paragraph 171) to check that filtering and monitoring is working on all school owned devices in all locations is met. The DSL, the Online Safety coordinator and the IT manager (or equivalent) will review the effectiveness of the filtering and monitoring system, looking at the records of the checks. Such a review will occur annually, however a further review will occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, adult content using the Internet Watch Foundation's list. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil or member of staff should speak to the IT Manager. The Online Safety Coordinator and DSL will then consider the request and record the outcome in writing.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals to be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, the Online Safety Coordinator / IT Staff will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSL immediately. Teaching staff should notify the Online Safety Coordinator, their Head of Department and the DSL if they are teaching material which might generate unusual internet traffic activity.

3.1.1 STAFF

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to the DSL immediately in line with the Child Protection and Safeguarding Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content. If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to the DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify the Online Safety Coordinator if they believe that appropriate teaching materials are being blocked.

3.1.2 PUPILS

Pupils must report to a trusted adult anything that they encounter online that makes them anxious, worried or upset (this includes accidental access to materials of a violent or sexual nature or that are otherwise inappropriate). Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact their form teacher or the Online Safety Coordinator for assistance.

3.2 EDUCATION AND TRAINING

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school.

All teaching staff (and relevant support staff) receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff and contractors receive information about Online Safety as part of their safeguarding briefing on arrival at school.

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. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Child Protection Policy and Safeguarding Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to the school's DSL.

3.2.1 THE TEACHING OF ONLINE SAFETY: PUPILS

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

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 and RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils are taught to recognise online sexual exploitation, stalking and grooming behaviour, the risks associated with these behaviours, and of their duty to report any such

instances they or their peers come across. Pupils can report concerns to the DSL/ Online Safety Coordinator or any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet such as those that apply to data protection, online safety and intellectual property. Pupils are taught about how to keep their own data secure and about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Child Protection and Safeguarding, Anti Bullying and Behaviour policies, which describe preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, or their parents for advice or help if they experience problems when using the internet and related technologies.

Appendix 2 sets out the outline of the school's Scheme of Work for teaching Online Safety.

3.2.2 PARENTS

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The school will contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings and talks for parents when an outside specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity. It also shares tips and safety information via newsletters.

3.3 USE OF PERSONAL DEVICES

3.3.1 STAFF

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted to protect data stored on them.

Staff are referred to the staff Code of Conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Old Buckenham Hall School are permitted to bring in personal devices for their own use. The exception to this are Meta (smart) glasses which may not be used onsite by pupils, staff, parents or visitors. Staff are not allowed to have their personal devices switched on during the working day (only during breaks and lunchtimes). They may use such devices in the main school staffroom or in staff offices. They may not use them in classrooms or other areas occupied by pupils.

Staff may not take personal devices with image taking capabilities including smart watches, META (smart) glasses, mobile phones, digital cameras, laptops and tablets into the Early Years setting. These devices must be kept securely in staff accommodation and may only be used in staff only areas where pupils are not present.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, IT Acceptable Use, Staff Code of Conduct and School Trips policies.

3.3.2 PUPILS

Pupils are not permitted to bring their own devices (laptops, tablets, chrome books, kindles, mobile phones, smart watches, smart glasses) to school. The exception to this are:

- boarders may bring a mobile phone to school. Pupils' phones must be handed in to boarding staff who will issue them at agreed times to enable children to call their parents.
- pupils with medical conditions e.g. pupils with diabetes who use a mobile phone to help monitor and control their condition (this will be discussed with parents and the pupil when the medical care plan is drawn up/reviewed).
- pupils may be allowed to take their mobile phones on some trips and visits. The decision to allow this rests with the trip leader and the Head. The risks associated with this will be accounted for in the risk assessment for the trip and appropriate mitigations put in place.

International pupils who need a mobile phone for use in an emergency during the journey to or from school are required to hand it to the Head of Boarding on arrival and collect it from him on departure. Phones must be switched off during the day. Any contact between the pupil and home during the day should be via the school office.

No personal devices including phones, cameras, laptops, tablets, smart watches, smart glasses, kindles belonging to pupils may be used during lessons.

The school issues some school owned devices to pupils. e.g. laptops to children with a SEND in Year 3 and above with a demonstrable need identified by the SENCo. The arrangements for issuing and collecting these devices are co ordinated by the SENCo. Devices are collected from the learning success department and returned each evening by the pupils. Pupils are aware of the Acceptable Use policy which is printed in their planners.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School's Behaviour Policy.

3.3.3 PARENTS

META (smart glasses) may not be worn or used on school premises. This applies to all stakeholders: parents, staff, pupils and visitors.

Parents may not use any personal device with image taking capacity in the Early Years setting. These include laptops, tablets, chrome books, kindles, mobile phones, smart watches, smart glasses. The only exception to this is if the Head of Pre-Prep or the Head give consent for parents to take pictures of their own child during a school event to which parents have been invited. Parents are reminded that they do not have consent to post images that include other people's children online and that they should refrain from doing so. Further guidance is included in the Taking, Storage and Use of Images Policy.

Parents of children in Form 1 to Form 5 are asked to refrain from using personal devices on school premises. We understand that sometimes parents will wish to photograph their child/children participating in school events to which parents have been invited. Parents are reminded that they do not have consent to post images that include other people's children online and that they should not do so. Further guidance is included in the Taking, Storage and Use of Images Policy.

3.3.4 VISITORS

META (smart) glasses may not be worn or used on school premises. This applies to all stakeholders: parents, staff, pupils and visitors. Visitors are asked not to use personal devices whilst on school premises without the permission of the Head.

3.4 ONLINE COMMUNICATIONS

3.4.1 STAFF

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Staff may not contact a pupil or parent / carer / recent alumni (i.e. pupils over the age of 13 who have left the school within the past eight years or parents of recent alumni using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers and recent alumni. Staff may not contact a pupil or parent / carer and recent alumni using a personal telephone number, email address, or other messaging system nor should pupils, parents and recent alumni / their parents / carers be added as social network 'friends' or similar. Staff who have children who attend the school may contact other parents to make social arrangements for their children. However, they should make the Head aware of these personal relationships and be careful to preserve professional boundaries and confidentiality at all times.

Staff must immediately report to [the DSL / 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT Manager.

3.4.2 PUPILS

All pupils are issued with their own personal school email addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work, assignments, research projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work, research purposes, pupils should contact IT Manager for assistance.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to the [the Online Safety Coordinator / DSL].

3.5 USE OF SOCIAL MEDIA

3.5.1 STAFF

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching or in the presence of pupils. Such access may only be made from staff members' own devices whilst in the staff room /staff-only areas of school.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring Old Buckenham Hall School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - using social media to bully another individual; or
 - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

3.5.2 PUPILS

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils very seriously and incidents will be dealt with under the Behaviour, Child Protection and safeguarding and Anti-Bullying policies as appropriate.

3.6 DATA PROTECTION

Please refer to the Data Protection policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work on their school device or to the school's One Drive as per the IT Acceptable Use Policy.

Staff devices should be encrypted if any data or passwords are stored on them. Removable devices are a cyber security risk and their use is generally not permitted. The school expects any removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

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 the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager in accordance with the [Data Protection Policy and IT Acceptable Use Policy].

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager.

3.7 PASSWORD SECURITY

Pupils and staff have individual school network logins and email addresses and storage folders. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers);
- not write passwords down; and
- not share passwords with other pupils or staff.

3.8 SAFE USE OF DIGITAL AND VIDEO IMAGES

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 / carers 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 and may be altered using AI to create pornography and deep fakes. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own personal images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

For further details please see the Taking, Storing and Use of Images Policy.

3.9 ARTIFICIAL INTELLIGENCE

Old Buckenham Hall School will evaluate the benefits and risks of any proposed use of generative AI by staff or pupils, with particular regard to risk associated with safeguarding, data protection and the possibility of bias and discrimination. Any approved use of AI will be kept under review and the school will remain alert to the possibility of unauthorised use.

Any usage of generative AI tools such as CoPilot is only permitted in the circumstances outlined in the School's AI policy, and subject to any conditions imposed by that policy.

In particular, personal or confidential information should not be entered into generative AI tools. This technology can potentially store and/or learn from data inputted and you should consider that any information entered into such tools is released to the internet.

It is also important to be aware that the technology, despite its advances, still produces regular errors and misunderstandings and should not be relied on for accuracy. In particular, pupils should not use these tools to answer questions about health / medical / wellbeing issues, or indeed anything of a personal nature. It is always best to seek help and recommendations as to reliable resources from a member of staff / the DSL.

3.10 MISUSE

Old Buckenham Hall School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity, they should report it to the DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

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 Safeguarding and Child Protection and Behaviour policies.

3.11 COMPLAINTS

As with all issues of safety at Old Buckenham Hall 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. Complaints should be addressed to the Online Safety Coordinator in the first instance, who will liaise with the senior leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Child Protection and Safeguarding Policy and reported to the school's Online Safety Coordinator and the DSL, in accordance with the school's Child Protection Policy and Safeguarding policy.

4. POLICY OWNER

This policy is owned by the Group Director of Safeguarding, Charlotte Marten cm1@rugbyschool.net

5. RELATED POLICIES AND GUIDANCE

In addition to the guidance identified in 1.2, this policy is linked to:

The Child Protection and Safeguarding Policy
The Taking, Storage and Use of Images Policy
The Acceptable Use of AI Policy
The Prevent Policy
The Behaviour Policy
The staff Code of Conduct
The Acceptable Use of IT User Agreement (Staff)
The Acceptable Use of IT User Agreement (Pupils)
Data Protection Policy and Privacy Notice/s;

School Trips Policy
PSHE / RSE Policy

APPENDIX 1**SANCTIONS IN RELATION TO THE MISUSE OF IT**

Examples of pupil incidents are outlined in the below table, along with a possible response. However, each incident will be reviewed on a case-by-case basis and the sanction will be dependent on the seriousness of the offence.

Examples of Pupil Incidents	Issue a Verbal Warning	Issue a Minus	Restriction of technology and network/internet access rights – ‘Teachers’ Request	Further sanction e.g. suspension/exclusion
Unauthorised use of non-educational sites during lessons	x			
Unauthorised/inappropriate use of social media/ messaging apps/personal email		x		
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device				x
Unauthorised downloading or uploading of files				x
Deliberately accessing or trying to access material that could be considered illegal (see list in “User Actions” section).				x
Deliberately manipulating media to misrepresent a person or their actions				x
Allowing others to access School network by sharing username and passwords				x
Attempting to access or accessing the School network, using another pupil’s account, or the account of a member of staff.				x
Corrupting or destroying the data of other users			x	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature				x
Actions which could bring the School into disrepute or breach the integrity of the ethos of the School			x	
Using proxy sites or other means to subvert the School’s filtering system				x

Deliberately accessing or trying to access offensive or pornographic material				x
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			x	
Sharing (including 'showing') video, photographic or audio recordings of others with the result to humiliate, mock or offend.				x
Making covert video or audio recordings or taking photographs of others without their knowledge or consent.			x	

APPENDIX 2 ONLINE SAFETY TEACHING AT OLD BUCKENHAM HALL SCHOOL

In delivering the online safety curriculum, provision will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities (SEND).

Year 1 & 2

Pupils will be taught:

- **Being Kind Online:** understanding how to interact respectfully, politely, and thoughtfully with others in digital environments.
- **Breaks from Screens:** recognising the importance of managing screen time to protect physical well-being, rest, and eye health.
- **Accessing Sites & Online Shows:** knowing to consult and obtain permission from a trusted adult before opening new apps, websites, or video content.
- **Why We Use Passwords:** understanding how secret credentials protect personal data and privacy online.

Years 3–6

Pupils will be taught:

- **CEOP Jessie & Friends:** navigating photo sharing, personal details, and online communications safely using structured framework tools.
- **Recognising Fake Emails & Age Ratings:** identifying suspicious messages, spam, and understanding age suitability guidelines across apps and games.
- **SMART Rules:** embedding essential digital safety habits and principles into everyday online use.
- **Scamming, Hacking & Staying Safe Online:** identifying security risks, securing devices, and protecting accounts against unauthorised access.
- **Social Media & Online Identity:** exploring digital footprints, online presence, and appropriate behavior within virtual communities.
- **Artificial Intelligence (AI):** exploring how AI systems work, their practical benefits for learning and daily life, and the risks surrounding data privacy, accuracy, and overuse.

Years 7–8

Pupils will be taught:

- **Social Media & Digital Footprints:** assessing how online contributions shape reputation and understanding the long-term impact of digital records.

- **Online Privacy & Data Protection:** managing privacy configurations and safeguarding personal data across digital platforms.
- **Cyberbullying & Unsafe Online Behaviours:** identifying digital harassment, understanding its motivation and impact, and recognising red flags in online interactions.
- **Online Scams, Phishing & Deception:** spotting deceptive practices, financial fraud, identity threats, and unsafe links.
- **Misinformation & Fake News:** evaluating online content critically to identify inaccuracies, bias, and false information.