Oakhyrst Grange School

Online Safety Policy

Date Reviewed:	15.09.2025, 19.01.26
Next Review Date:	01.09.2026
Policy Owner:	Margarita Gorman
Ratified @ FGB/Committee Name & Date:	F&E 30.09.2024 FGB 14.10.2024

Mission Statement

We are committed to providing a supportive, enjoyable and family style environment in which every child is nurtured and encouraged to achieve their potential through a broad-based curriculum and opportunities for developing sporting, dramatic, artistic and musical talents.

Statement of Aims & Objectives

- To enable each child to fulfil their own academic and personal potential.
- To instil in every child the importance of developing personal initiative and to foster in them a belief that they can fulfil their potential in any area of school life.
- To provide a broad based academic and extra-curricular education that is delivered in such a way as to satisfy the learning needs of each and every pupil.
- To help each pupil to develop both a set of Christian values and an understanding and appreciation of other religious beliefs.
- To learn the difference between right and wrong and to appreciate that rights and responsibilities are equally balanced.
- To develop and promote a sense of caring and community between the pupils within the school and the wider community as a whole.
- To instil in each pupil a high degree of self-respect and respect for their fellow pupils, teachers and other adults.
- To prepare each child for the transition to the next stage of their education and to be able to take advantage of any opportunities as they present themselves.

Safeguarding

Oakhyrst Grange School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. At this school we respect and value all children and are committed to providing a caring, friendly and safe environment for our pupils so that they can learn in a relaxed and secure atmosphere. We believe that every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Oakhyrst Grange School. We recognise our responsibility to safeguard all who access school and promote the welfare of all of our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying. This should be read in conjunction with the Safeguarding Policy.

All staff will be asked to complete training annually following KCSIE updates. Further safeguard training will take place throughout the year. All staff must wear their lanyards at all times.

The Safeguarding governor is: Pauline Clark Pauline.clark@oakhyrstgrangeschool.co.uk

DSL: Roxann Dowling (Head of EYFS)

DDSL: Gemma Mitchell (Headteacher)

DDSL: Faye Dance (Deputy Headteacher)

Telephone: 01883 343344

Safeguarding Team: DSL@oakhyrstgrangeschool.co.uk

Key People

Curriculum leads with relevance to Online Safeguarding and their role	Miss Lara Sumners (PSHE)
Online Safety Officer	Margarita Gorman
IT Technical Co-ordinator	Margarita Gorman
IT Managed Services Provider	Cygnet IT Services

Contents

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with ‘Keeping Children Safe in Education’ 2025 (KCSIE), ‘Teaching Online Safety in Schools’, statutory RSHE guidance and other statutory documents. It is cross-curricular (with relevance beyond Relationships, Health and Sex Education, Citizenship and Computing) and designed to sit alongside Oakhyrst Grange School’s statutory Child Protection & Safeguarding Policy. Any issues and concerns with online safety MUST always follow the school’s safeguarding and child protection procedures.

Main online safety risks in 2024/2025

Current online safeguarding trends (Nationally)

Last year, it was highlighted the rapid rise of generative AI (GenAI). Since then, the trend has exploded. Thousands of sites now offer AI-generated content, including disturbing levels of abusive, pornographic, and even illegal material like child sexual abuse content. Some platforms host AI “girlfriends,” unregulated therapy bots, and even chatbots that encourage self-harm or suicide—tools many pupils can access freely at home or school. Chatbots can also blur reality, offering harmful advice or engaging in sexualised and bullying conversations. Their addictive design and unmoderated nature heighten the risk of overuse and exploitation.

When used for generating text, GenAI presents multiple risks. It can spread misinformation, facilitate plagiarism, and most worryingly, bypass safety settings. Many tools lack effective age controls and produce inappropriate content.

Beyond text, GenAI makes it easier than ever to create sexualised images and deepfake videos. These can have a devastating emotional and physical impact on young people, including blackmail and abuse. The Internet Watch Foundation has warned of a sharp rise in AI-generated child sexual abuse imagery. Alarming reports also show children using nudifying apps to create illegal content of peers.

It’s critical to stress that in the UK, *any* CSAM (child sexual abuse material)—AI-generated, photographic, or even cartoon—is illegal to create, possess, or share.

Ofcom’s ‘Children and parents: media use and attitudes report 2025’ has shown that YouTube remains the most used site or app among all under 18s, followed by WhatsApp, TikTok, Snapchat and Instagram. With children aged 8-14 spending an average of 2 hours 59 minutes a day online across smartphone, tablet and computer – with girls spending more time online than boys, four in ten parents continue to report finding it hard to control their child’s screen time. Notably, 52% of 8-11s feel that their parents’ screen time is also too high, underlining the importance of modelling good behaviour.

Given the 13yrs+ minimum age requirement on most social media platforms, it is notable that over half of 3-12-year olds (55%) were reported using at least one app. Despite age restrictions, four in ten admit to giving a fake age online, exposing them to content inappropriate for their age and increasing their risk of harm, with over a third of parents of all 3-17s saying they would allow their child to have a profile on sites or apps before they had reached the minimum age.

As a school we recognise that some of our pupils are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore will remind about best practice while remembering the reality for most of our pupils is quite different.

This is striking when you consider that 25% of 3 to 4-year olds have access to their OWN mobile phone (let alone shared devices), rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, even 3- to 6-year-olds are being tricked into ‘self-generated’ sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and for the first time, there were more 7-10-year-olds visible in child sexual abuse material (CSAM) images than 11-13s.

Growing numbers of children and young people are using social media and apps, primarily TikTok as their source of news and information, with little attention paid to the facts or veracity of influencers sharing news.

There have also been significant safeguarding concerns where parents have filmed interactions with staff outside the school gates and posted this on social media, putting children and the wider school community at risk of harm.

Cyber Security is an essential component in safeguarding children and features within KCSIE. Sadly, the education sector remains a clear target for cyber-attacks, with the Cyber Security Breaches Survey 2025 reporting high levels of schools being attacked nationally, with 60% of secondary schools and 44% of primary schools reporting a breach or attack in the past year.

Introduction

This policy is to safeguard and protect all members of the Oakhyrst Grange School community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. The Oakhyrst Grange School community includes, teaching, supply and support staff, governors, volunteers, contractors, pupils, parents/carers, visitors and community users who have access to and are users of the Oakhyrst Grange School digital technology, networks and systems both on-site and remotely, and at any time, or who use technology in their school role.

This policy aims to promote a whole school approach to online safety by:

- Setting out expectations for all Oakhyrst Grange School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- Helping safeguarding and Senior Leadership Team (SLT) to have a better understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. filtering and monitoring), curriculum leads (e.g. PSHE) and beyond.
- Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.
- Facilitating the safe, responsible, respectful and positive 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.
- Helping 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, and
  - their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice.
  - the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession.
- Establishing clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time. All staff have a key role to play in feeding back on potential issues.

Depending on their role, all members of the school community should **read the relevant section in Appendix 1 of this document** that describes individual roles and responsibilities. Please note there is one for All Staff which MUST be read even by those who have a named role in another section. There is also pupil, governor, etc. role descriptions in Appendix.

Education and Curriculum

Despite the risks associated with being online, Oakhyrst Grange School recognises the opportunities and benefits of children too. Technology is a fundamental part of our adult lives and so developing the competencies to understand and use it, are critical to children's later positive outcomes. The choice to use technology in school will always be driven by pedagogy and inclusion. We currently use technology like iPads, reading pens, recording like speech to text etc. to support differentiation and inclusion in the curriculum.

Pupil Online Safety curriculum

Oakhyrst Grange School has a clear, progressive online safety education programme as part of the PSHE and other curriculum areas as relevant. This covers a range of skills to develop competencies (as well as knowledge about risks) and builds on what pupils have already learned and identifies subject content that is appropriate for their stage of development.

As well as teaching about the underpinning knowledge and behaviours that can help pupils navigate the online world safely and confidently regardless of the device, platform or app, we embed teaching about online safety and harms through a whole school approach and provides an understanding of these risks to help tailor teaching and support to the needs of the pupils.

- Staff should also 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.
- When overseeing the use of technology (devices, the internet, generative AI tools etc.) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of tasks.
- All staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including extra-curricular, extended school activities if relevant and remote teaching, supporting them with search skills, reporting and accessing help, critical thinking (e.g. disinformation, misinformation, and conspiracy theories in line with KCSIE 2025), access to age-appropriate materials and signposting, and legal issues such as copyright and data law.
- Annual reviews of curriculum plans / schemes of work (including for SEND pupils) take place and are used as an opportunity to look more closely in keys areas such as Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling Online Safety Concerns and Incidents

It is vital that all staff recognise that online safety is a part of safeguarding and so concerns must be handled in the same way as any other safeguarding concern. Safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should speak to the Safeguarding Lead with any concerns, no matter how small these seem, to contribute to the overall picture or highlight what might not yet be a problem.

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

Handling and Managing Incidents

School procedures for dealing with online safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Sexual Harassment / Child-on-Child Abuse Policy
- Anti-Bullying Policy

- Behaviour Policy (including school sanctions)
- Acceptable Use Agreement
- Prevent Risk Assessment / Policy
- Privacy Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc.)

Oakhyrst Grange School commits to take all reasonable precautions to safeguard pupils online, but recognises that incidents will occur both inside school and outside 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 Online Safety Officer and/or Designated Safeguarding Lead on the same day. The reporting member of staff will ensure that a record is made of the concern on CPOMs and this includes any concerns raised by the filtering and monitoring systems.

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

The school will actively seek support from other agencies as needed (i.e. the local authority, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF and Harmful Sexual Behaviour Support Service). The DfE guidance Behaviour in Schools, advice for headteachers and school staff September 2024 provides advice and related legal duties including support for pupils and powers of staff when responding to incidents – see pages 31-33 for guidance on child on child sexual violence and harassment, behaviour incidents online and mobile phones.

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 concerning or breaks the law.

We will ensure all online safety reporting procedures are sustainable for any unforeseen periods of closure.

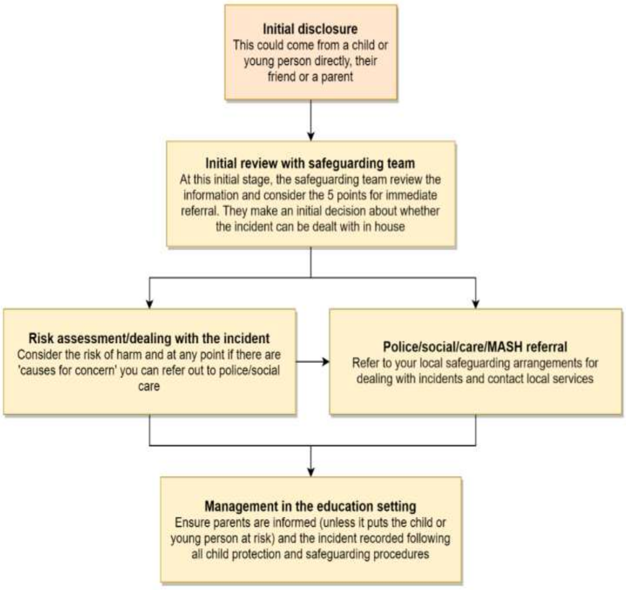
Nudes – Sharing nudes and semi-nudes

Oakhyrst Grange School refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings

A one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the DSL or Online Safety Officer to first become aware of an incident, and it is vital that the correct steps are taken. **Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.**

It is important that everyone understands that whilst the sharing of nudes involving children is illegal, pupils should be encouraged and supported to talk to members of staff if they have made a mistake or had a problem in this area. The UKCIS guidance seeks to avoid unnecessary criminalisation of children.

The school DSL will use the full guidance document, Sharing nudes and semi-nudes: advice for education settings to decide next steps and whether other agencies need to be involved (See flowchart below from the UKCIS guidance) and steps regarding liaising with parents and supporting pupils.



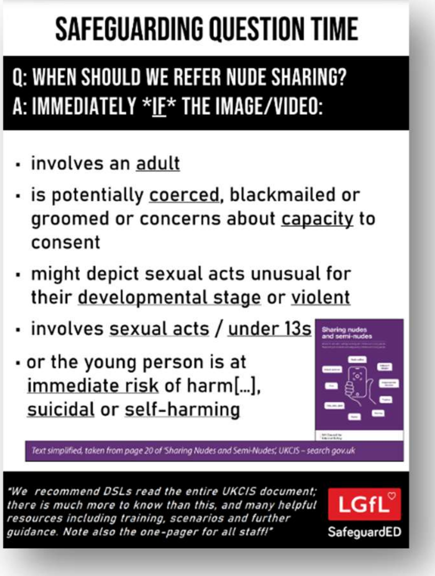
Initial disclosure
This could come from a child or young person directly, their friend or a parent

Initial review with safeguarding team
At this initial stage, the safeguarding team review the information and consider the 5 points for immediate referral. They make an initial decision about whether the incident can be dealt with in house

Risk assessment/dealing with the incident
Consider the risk of harm and at any point if there are 'causes for concern' you can refer out to police/social care

Police/social/care/MASH referral
Refer to your local safeguarding arrangements for dealing with incidents and contact local services

Management in the education setting
Ensure parents are informed (unless it puts the child or young person at risk) and the incident recorded following all child protection and safeguarding procedures



SAFEGUARDING QUESTION TIME

Q: WHEN SHOULD WE REFER NUDE SHARING?
A: IMMEDIATELY *IF* THE IMAGE/VIDEO:

- involves an adult
- is potentially coerced, blackmailed or groomed or concerns about capacity to consent
- might depict sexual acts unusual for their developmental stage or violent
- involves sexual acts / under 13s
- or the young person is at immediate risk of harm[...], suicidal or self-harming

Text simplified, taken from page 20 of 'Sharing Nudes and Semi-Nudes', UKCIS – search gov.uk

"We recommend DSLs read the entire UKCIS document; there is much more to know than this, and many helpful resources including training, scenarios and further guidance. Note also the one-pager for all staff!"

LGfL SafeguardED

Upskirting

Upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child on child abuse pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying, including incidents that take place outside school or from home should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

It is important to be aware that sometimes fights are being filmed, live streamed or shared online and fake profiles are used to bully children in the name of others. When considering bulling, staff will be reminded of these issues.

Child-on-child Sexual violence and harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures governing pupils and adults use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Agreement as well as in this document.

Where pupils contravene these rules (same applies for any home learning), the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the Staff Code of Conduct.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

Social media incidents involving pupils are often safeguarding concerns and should be treated as such and staff should follow the Safeguarding and Online Safety Policy.

Breaches will be dealt with in line with the school Behaviour policy (for pupils) or Code of Conduct (for staff). See also the social media section later in this document for rules and expectations of behaviour for children and adults in the Oakhyrst Grange school community. These are also governed by school Acceptable Use Agreements.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Oakhyrst Grange School will request that the post be deleted and will expect this to be actioned promptly.

Where an offending post has been made by a third party, the school may report it to the platform it is hosted on, and may contact the Professionals' Online Safety Helpline, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Extremism

Oakhyrst Grange school has obligations relating to radicalisation and all forms of extremism under the Prevent Duty. Staff will not support or promote extremist organisations, messages or individuals, give them a voice or opportunity to visit the school, nor browse, download or send material that is considered offensive or of an extremist nature. We ask for parents' support in this also, especially relating to social media, where extremism and hate speech can be widespread on certain platforms.

Data protection and cybersecurity

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's Privacy policy that protects the privacy of personal information or data. It is important to remember that there is a close relationship between both data protection and cyber security and a school's ability to effectively safeguard children.

Schools should remember that data protection does not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in *Data protection in schools*, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2025, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.

Appropriate filtering and monitoring

The designated Safeguarding Lead (DSL) has lead responsibility for filtering and monitoring and works closely with IT technical coordinator and school authorised IT Managed Services Provider to implement the DfE filtering and monitoring standards, which require schools to:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provision at least annually.
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We look to provide ‘appropriate filtering and monitoring, as outlined in Keeping Children Safe in Education, at all times.

We ensure ALL STAFF are aware of filtering and monitoring systems and play their part in feeding back about areas of concern, potential for pupils to bypass systems and any potential over-blocking. They can submit concerns at any point via email to the Online Safety Officer or DSL and will be asked for feedback at the time of the regular checks.

Technical and safeguarding colleagues work together closely to carry out annual reviews and check and also to ensure that the school responds to issues and integrates with the curriculum.

At Oakhyrst Grange, we recognise that generative AI sites can pose data risks so staff are not allowed to enter pupil’s data and where they use them, they must be approved. Staff are only allowed to use AI for resources such as planning. For pupils, we block the generative AI category.

Safe Search is enforced on search engines on all school-managed Desktops. We recommend the use of Kiddle and Swiggle search engines for EYFS and KS1 children.

Our YouTube mode is unrestricted for Staff use only. Pupils do not have accessed to YouTube.

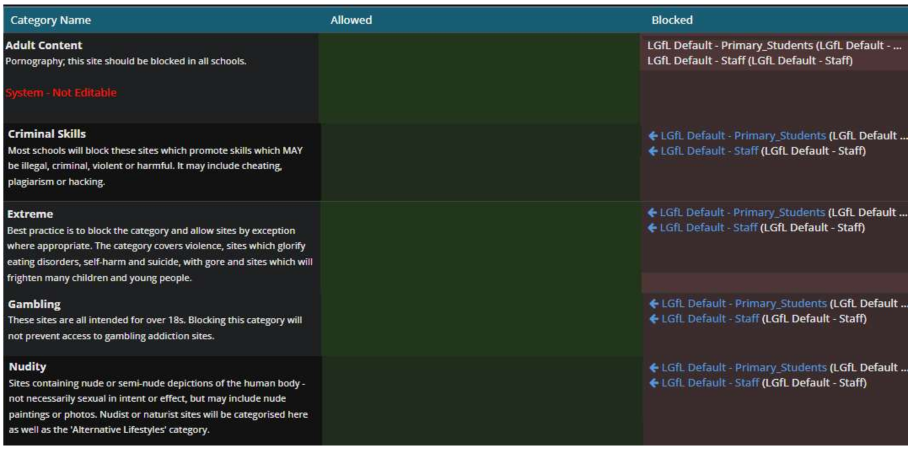
Currently, we do not have any out of hours policies. Filtering and monitoring are active 24 hours a day.

Staff will be reminded of the systems in place and their responsibilities at induction and start of year safeguarding, as well as via AUAs and regular training reminders, in the light of the annual review and regular checks that will be carried out. This will take place either in the form of emails or at staff meetings.

Internet Access, Security (Virus Protection) and Filtering

- Firewall protection provided by LGfL SchoolProtect
  SchoolProtect is a **highly flexible web filtering system** designed and built for the UK education sector, fulfilling the requirement of the Department for Education’s statutory safeguarding guidance ‘Keeping Children Safe in Education’ to offer ‘appropriate filtering’ – this is demonstrated by their self-certification to the UK Safer Internet Centre.
- With SchoolProtect, control is placed in the hands of schools & the system allows schools to exercise as much filtering control as they wish. Schools have the option to create their own policies, or simply adopt the default filtering policies specially created for educational sector.

Some of the categories currently blocked are:

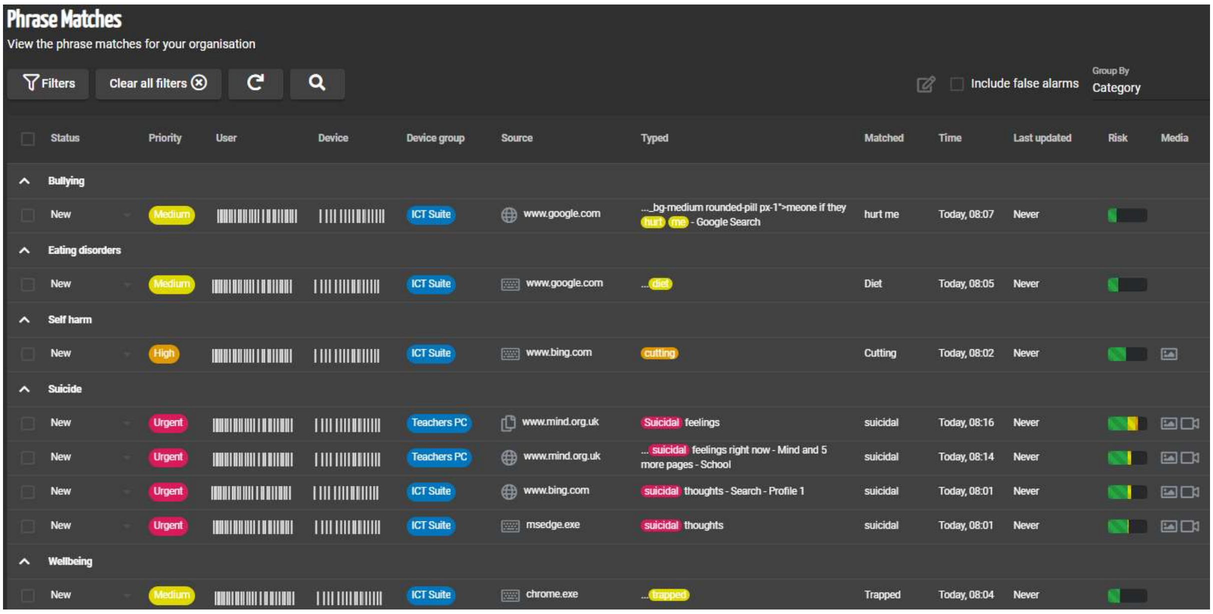


Category Name	Allowed	Blocked
Adult Content Pornography; this site should be blocked in all schools. System - Not Editable		LGfL Default - Primary_Students (LGfL Default - ... LGfL Default - Staff (LGfL Default - Staff)
Criminal Skills Most schools will block these sites which promote skills which MAY be illegal, criminal, violent or harmful. It may include cheating, plagiarism or hacking.		← LGfL Default - Primary_Students (LGfL Default ... ← LGfL Default - Staff (LGfL Default - Staff)
Extreme Best practice is to block the category and allow sites by exception where appropriate. The category covers violence, sites which glorify eating disorders, self-harm and suicide, with gore and sites which will frighten many children and young people.		← LGfL Default - Primary_Students (LGfL Default ... ← LGfL Default - Staff (LGfL Default - Staff)
Gambling These sites are all intended for over 18s. Blocking this category will not prevent access to gambling addiction sites.		← LGfL Default - Primary_Students (LGfL Default ... ← LGfL Default - Staff (LGfL Default - Staff)
Nudity Sites containing nude or semi-nude depictions of the human body - not necessarily sexual in intent or effect, but may include nude paintings or photos. Nudist or naturist sites will be categorised here as well as the 'Alternative Lifestyles' category.		← LGfL Default - Primary_Students (LGfL Default ... ← LGfL Default - Staff (LGfL Default - Staff)

- Network servers are protected by Sophos Intercept X for servers and desktop devices through the use of Sophos Central Intercept X Endpoint Advance anti-virus software. Mobile devices e.g. iPads are protected through Sophos Intercept X for Mobile.
- Systems are protected against malware and malicious software by ThreatDown (powered by Malwarebytes) which detects and removes malware and other advanced threats. It stops malware in real-time, before it can be a danger to the devices.
- Mail Protection/Filtering service by Microsoft.
- Uses Egress secure email/file for 'protect-level' (sensitive personal) data over the Internet.
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site.

Monitoring

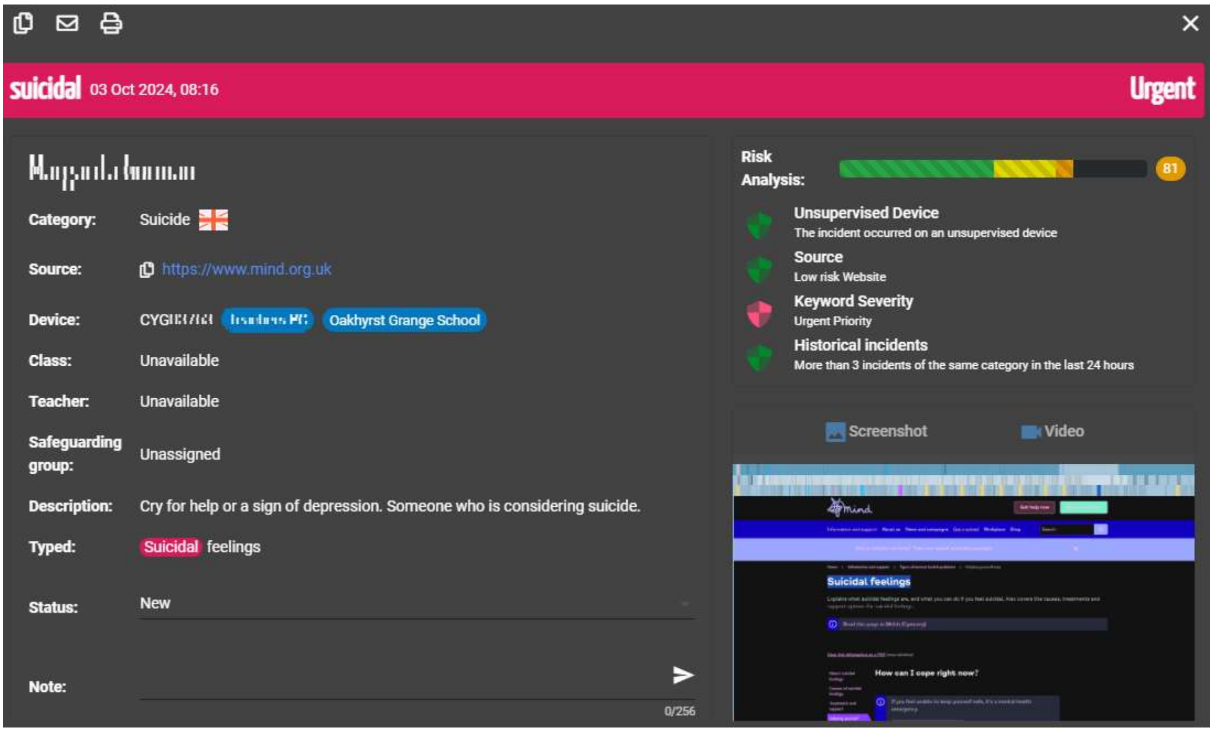
- Physically monitoring by staff watching screens of users.
- Has NetSupport Safeguarding and Online Safety Toolkit which helps to maintain a safe learning environment.
- Has NetSupport Classroom management and Instruction tools to help teachers to monitor real time class activities e.g. websites they are visiting, applications they are using, what they are typing etc. from the teacher's Desktop. This helps to keep children safe and on task.
- Has NetSupport Student Wellbeing module which includes keyword monitoring.
  - The keyword monitoring tool is driven by a pre-supplied online safety database of keywords and phrases that updates regularly and covers a wide range of topics from self-harm, bullying, racism and more. School can tailor the database to set risk levels for specific keywords or phrases that may be more important/appropriate to the age group.
  - The alert can be a simple text record for low level concern to screen shot or video recording for urgent and high alerts. The alerts provide school with information on any pupil that might suggest they may be engaged in activity that would place them at risk.



Phrase Matches

View the phrase matches for your organisation

Status	Priority	User	Device	Device group	Source	Typed	Matched	Time	Last updated	Risk	Media
Bullying											
New	Medium	[redacted]	[redacted]	ICT Suite	www.google.com	...._bg-medium rounded-pill px-1">meone if they hurt me - Google Search	hurt me	Today, 08:07	Never		
Eating disorders											
New	Medium	[redacted]	[redacted]	ICT Suite	www.google.com	...diet	Diet	Today, 08:05	Never		
Self harm											
New	High	[redacted]	[redacted]	ICT Suite	www.bing.com	cutting	Cutting	Today, 08:02	Never		
Suicide											
New	Urgent	[redacted]	[redacted]	Teachers PC	www.mind.org.uk	Suicidal feelings	suicidal	Today, 08:16	Never		
New	Urgent	[redacted]	[redacted]	Teachers PC	www.mind.org.uk	... suicidal feelings right now - Mind and 5 more pages - School	suicidal	Today, 08:14	Never		
New	Urgent	[redacted]	[redacted]	ICT Suite	www.bing.com	suicidal thoughts - Search - Profile 1	suicidal	Today, 08:01	Never		
New	Urgent	[redacted]	[redacted]	ICT Suite	msedge.exe	suicidal thoughts	suicidal	Today, 08:01	Never		
Wellbeing											
New	Medium	[redacted]	[redacted]	ICT Suite	chrome.exe	...trapped	Trapped	Today, 08:04	Never		



suicidal 03 Oct 2024, 08:16 Urgent

[redacted]

Category: Suicide

Source: https://www.mind.org.uk

Device: CYG[redacted] [redacted] Oakhyrst Grange School

Class: Unavailable

Teacher: Unavailable

Safeguarding group: Unassigned

Description: Cry for help or a sign of depression. Someone who is considering suicide.

Typed: Suicidal feelings

Status: New

Note:

0/256

Risk Analysis: 81

Unsupervised Device
The incident occurred on an unsupervised device

Source
Low risk Website

Keyword Severity
Urgent Priority

Historical incidents
More than 3 incidents of the same category in the last 24 hours

The DSL and Online Safety Officer checks filtering reports and notifications regularly and takes any necessary action as a result. Monitoring alerts are checked daily by the Online Safety Officer. Urgent and High alerts are sent to the DSL automatically via email notifications.

Cybersecurity

Our web filtering and wireless network are secured to industry and appropriate standards suitable for educational use. All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

There is a shared work area for pupils and separate one for staff. We do not allow any outside agencies to access our network remotely except where there is a clear professional need. The Headteacher approved such need and the access is audited/restricted and is only through approved systems.

User Accounts

No one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins.

Staff:

- An individual log-in for all staff to access to the school's network service.
- Guest accounts and Supply teacher accounts are occasionally used for external/short-term visitors. Supply teachers may be given temporary access to appropriate services.
- All users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a phishing scam, they must change their password and inform the school immediately.
- We implement multi-factor authentication where it is practicable to do so.
- Staff are responsible for ensuring that any computer/laptop, iPad or any other devices loaned to them by the school, is used primarily to support their professional responsibilities.

Password policy

Staff/Governors:

- All staff/governors have their own unique username and private passwords to access school systems and must always keep their passwords private and must not share with others. All staff/governors are required to change their passwords annually by the end of September.
- All staff/governors are advised to use STRONG passwords, a minimum of 8 characters that are a combination of letters (contains both uppercase and lowercase), numbers and symbols (@, #, $, %, etc.).
- We require staff using critical systems to use Multi-factor authentication (at least 2 or more verification factors).

Pupil:

- Pupils of Year 5 and Year 6 classes access to the school's network service is through a unique username and password.
- Pupils of Year 2 to 4 classes access to the school's network service is through a unique username and common password at the start of the school term and will gradually progress to unique password during the academic year.

Devices

Staff MUST:

- Devices must be signed out or locked whenever they are left unattended, regardless of the duration.
- All updates, including security and device-related updates, must be carried out promptly upon notification.
- Report lost or stolen equipment, including accessories, as soon as possible to the school. Change all account passwords at once when a device is lost or stolen and report immediately to the school.
- Report a suspected threat or security weakness in the school's systems to the school.

Sharing Files

Oakhyrst Grange School recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach users are required to:

- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites.
- Wherever possible, keeping Oakhyrst Grange School's files on school systems.
- Do not send school files to personal accounts.
- Verify the recipient of data prior to sending.
- Use file encryption where possible, sending passwords/keys via alternative communication channels.
- Alert the DPO/Headteacher to any breaches, malicious activity or suspected scams.

System Security

We will build security principles into the design of Oakhyrst Grange School's IT services.

- Security patching – network hardware, operating systems and software.

- Plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them.
- Actively manage anti-virus systems by the school's IT Managed Services Provider.
- Actively manage and test backups by the school's IT Managed Services Provider.
- Review and update security controls that are available with existing systems.
- Separate wireless networks used for visitors' & staff personal devices from school systems.

Backup

This school:

- A fully managed backup that is actively monitored and will automatically raise a ticket with the school authorised IT Managed Services Provider should a backup fail.
- The backup is encrypted at source and stored offsite (in UK data centres).
- Files and folders have daily backup with a 10 weeks retention period.
- Full Images have weekly backup with a 15 days retention period.
- Both file and folder backup and full image backup (for disaster recovery) with a 10 weeks retention policy as standard.

Messaging/commenting systems (incl. email, learning platforms etc.)

Authorised system

No pupils in school have an active email account. When ICT curriculum requires an email account, accounts are available temporary and restricted to emailing within the school and cannot email external accounts.

Coding Club pupils using Scratch online and it has a commenting section. An Information pack is provided to parents/carers about Scratch online. Pupils are reminded regularly they are not allowed to use the comment/likes/share project sections. Alerts can be viewed by the Coding club teacher.

Staff at Oakhyrst Grange communicate using a Microsoft 365 email/Teams account for all school emails. They never use a personal/private email account (or other messaging platform) to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.

Class teachers also have a SeeSaw Learning Platform account and Pre-Reception Class teacher with a Tapestry Learning Journal account for their professional use.

Use of a different platform must be approved in advance by the DPO/Headteacher. Any unauthorised attempt to use a different system may be a safeguarding concern or a disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).

- Use of any new platform or app with communication facilities or any child login or storing school/child data must be approved in advance by the school and centrally managed.
- Any systems above are centrally managed and administered by the school or school authorised IT Managed Services Provider. (i.e. they can be monitored/audited/viewed centrally; are not private or linked to private accounts). This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation. Check SeeSaw has an alternative teacher for they are not centrally managed
- Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from, or data being uploaded to the wrong account. If this a private account

is used for communication or to store data by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

Behaviour / Usage principles of messaging/commenting systems

- Protect-level' data should be transferred by Egress encrypted email. If there is no secure file transfer solution available for the situation, and the file must have password-protection enabled and have the authorisation of the Headteacher/DPO.
- Data protection principles will be followed at all times when it comes to all school communications, in line with the school Privacy Policy and only using the authorised systems mentioned above.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff.

Use of generative AI

At Oakhyrst Grange School we acknowledge that generative AI platforms (e.g. ChatGPT or the use of Co-Pilot create images and videos) are becoming widespread. We are aware of and follow the DfE's guidance on Generative AI in education. In particular:

- We will talk about the use of these tools with pupils, staff and parents – their practical use as well as their ethical pros and cons. AI topics are also part of our PSHE curriculum.
- We are aware that there will be use of these apps and exposure to AI creations on devices at home for some pupils – these experiences may be both positive/creative and also negative (inappropriate data use, misinformation, bullying, deepfakes, undressing apps).
- The use of any generative AI in Exams, or to plagiarise and cheat is prohibited.
- We currently allow the use generative AI, e.g. ChatGPT orCo-Pilot, by staff for their professional use in school only for information or resources. However, staff should be aware of misinformation, data privacy implications and intellectual property rights to the original content.
- Pupils currently do not use generative AI in lessons due to their age and also the difficulty in filtering/monitoring these platforms which may create inappropriate material and do not have safety settings.

Online storage or learning Platforms

All the principles outlined above also apply to any system to which you log in online to conduct school business, whether it is to simply store files or data (an online 'drive') or collaborate, learn, teach, etc. In Oakhyrst Grange School this includes Microsoft's Office 365 including OneDrive, Google Workspace including Google Drive, SeeSaw Learning Platform and Tapestry Learning Journal, BOFA/Atom Learning.

It is important to consider data protection and cyber security before adopting such a platform or service and at all times when using it.

The following principles apply:

- The Headteacher/DPO approves new cloud systems and platforms.

- Staff are only given access when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Pupil images and videos are only made public with parental permission.
- Only school-approved platforms are used by pupils or staff to store pupil work.
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

School website

The school website is a key public-facing information portal for the school community with reputational value. The Headteacher and the Governors take day-to-day responsibility to updating the content that the website content is accurate and compliant.

The site is managed and hosted by Innermedia.

Where staff submit information for the website, they are asked to remember that schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited, and material only used with permission. There are many open-access libraries of public-domain images/sounds etc that can be used. Finding something on Google or YouTube does not mean that copyright has been respected.

Digital Images and Video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for the purpose of

- Advertising
- Websites
- Social Media

Whenever a photo or video is taken/made, the member of staff taking it will check the latest information on our Management Information System (MIS iSAMS) before using it for any purpose.

Any pupils shown in public facing materials are never identified with more than first name and photo file names/tags do not include full names to avoid accidentally sharing them.

All staff are governed by the school's Acceptable Use Agreement, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored. No member of staff will ever use their personal phone to capture photos or videos of pupils. However, with the explicit permission of the Headteacher, staff may occasionally allow to use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services.

Photos are stored on the school network and a password protected external drive in line with the retention schedule of the school Data Privacy Policy.

Staff and parents are reminded at the start of a school event or production about the importance of not sharing images on social media or otherwise without permission, due to reasons of child protection e.g. children who are looked after by the local authority may have restrictions in place for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy.

We encourage staff and pupils to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing over-sharing (or providing embarrassment in later life – and it is not for us to judge what is embarrassing or not).

Pupils are taught about how images can be manipulated in their ICT and online safety lesson. Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Social Media

Oakhyrst Grange School's SM presence

Oakhyrst Grange School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint. (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'Googling' the school and negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and may respond to criticism and praise in a fair, responsible manner. We conduct regular checks of privacy and security settings on social media accounts to ensure appropriate access.

Social Media Lead is responsible for managing our Facebook and Instagram social media accounts and checking our Wikipedia and Google reviews and other mentions online.

Staff, pupils' and parents' SM presence

Social media, including all apps, sites and games that allow sharing and interaction between users, is a fact of modern life. As a school, we accept that many parents, staff and pupils will use it. However, as stated in the Acceptable Use Agreements which all members of the school community signed, 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 and we ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

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; with whom, for how long, and when. We encourage parents to sign up to the school's subscribed The National College (formerly National Online Safety) Website for information e.g. What Parents need to know guides, annual award/certificate in online safety/reputation. Information on how to join The National College website are given to parents at the start of each academic year, in the half-termly newsletter or you can request the information again by emailing the school's office.

Although the school has an official Facebook and Instagram account and will respond to general enquiries about the school, we ask parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils. We also use the Seesaw learning platform and Tapestry to communicate schoolwork with parents/pupils.

Pupils are not allowed* to be 'friends' with or make a friend request** to any staff, governors, volunteers and contractors or otherwise communicate via social media.

Pupils are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. 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 Headteacher, 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 Headteacher (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 or its stakeholders 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.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there has been a considerable number of Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

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. See the Digital Images and Video section of this policy and permission is sought before uploading photographs, videos or any other information about other people. Parents must **not** covertly film or make recordings of any interactions with pupils or adults in schools or near the school gates, nor share images of other people's children on social media as there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of children for internal purposes such as recording attainment, but it will only do so publicly if parents have given consent on the relevant form.

Device usage

AUAs remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with those AUAs and the sections of this document which impact upon device usage, e.g. copyright, data protection, social media, misuse of technology, and digital images and video.

All staff who work directly with children

Personal devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personal devices.

Personal mobile phone should be kept on silent, out of sight and only use in private staff areas during school hours.

Mobile devices with camera e.g. iPads are not permitted to be used in certain areas within the school, e.g. changing rooms and toilets.

If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.

Child/staff data should never be downloaded onto a private phone.

Staff, including peripatetic music staff and dance teachers who wish to use their personal mobile device for teaching purposes only (e.g. accompanying music, metronome app and audio recordings for assessments) must seek permission and a written approval from the Headteacher. (See Appendix 3a – Request to use personal mobile device in school).

Staff are not permitted to use their own mobile devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Pupils

No pupils should bring his or her mobile device, including smart watches into school. Any device brought into school will be confiscated. However, the School accepts that there may be particular circumstances in which a parent/carer wishes their child to have a mobile phone for their own safety, e.g. walk home on their own after school, or to monitor health conditions, Parent/carer(s) must confirm this intent in writing and approved by the Headteacher. These phones may be kept by the pupil (for monitor health conditions) or stored in the office and be collected by the pupil at the end of the day.

If a pupil breaches the Online Safety Policy then the mobile device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers at the end of the day.

Volunteers, Contractors, Governors

Should leave their phones in their pockets. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.

Parents

Parents are asked to leave their phones in their pockets. They can ask permission to access the guest wireless network but have no access to the networked files/drives and subject to the Acceptable Use Agreement (AUA) and all internet traffic is monitored.

They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school productions or events, please refer to the Digital images and video section of this document.

Storage, Synching and Access

School owned mobile devices (e.g. iPads):

- The devices should only be accessed with a school owned account.
- The devices are stored in a secure charging cabinet or a locked drawer/cabinet.
- The device has a school created account and all apps and file use is in line with this policy.
- No personal elements may be added to this device.
- If a personal account is to be used:
  - Staff must seek permission from the Headteacher.
  - Exit process – when the device is returned, the staff member must log in with the personal ID so that the device can be Factory Reset and cleared for reuse.

Use of school devices

Staff and pupils are expected to follow the terms of the school acceptable use agreement for appropriate use and behaviour when on school devices, whether on site or at home. School devices are not to be used in any way which contravenes AUAs, behaviour policy / Staff Code of Conduct.

Wi-Fi is accessible to Staff and Guest for school-related internet use and/or limited personal use within the framework of the acceptable use agreement. All such use may be monitored.

School devices for staff or pupils are restricted to the apps/software installed by the school, whether for use at home or school, and may be used for learning and reasonable appropriate personal use. If staff wish to have any other software installed on school device(s), it must be explicitly approved by the school (See Appendix 2b).

Staff are given either an encrypted USB drive or DataShur USB drive to use on all school devices. No other USB drives are allowed unless they are virus checked and approved by the school.

All and any usage of devices and/or systems and platforms may be tracked.

Trips / events away from school

For school trips/events away from school, teachers may be issued a school duty phone and this number used for any authorised or emergency communications with pupils and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the Headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or pupil accessing a teacher’s private phone number.

Searching and confiscation

In line with the DfE guidance, the Headteacher and staff authorised have a statutory power to search pupils/property on school premises Searching, screening and confiscation in schools - GOV.UK. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying. Pupils are not allowed to have mobile phones at school.

Reference: London Grid for Learning
Reference: NetSupport Classroom.Cloud

This Policy is subject to regular review.

Appendix 1 – Roles

Please read the relevant roles & responsibilities section from the following pages.

School staff – note that you may need to read two sections – if your role is reflected here, you should still read the "**All Staff**" section.

Roles:

- All Staff
- Headteacher
- Designated Safeguarding Lead (DSL) / Online Safety Officer
- Governing Body, led by Online Safety / Safeguarding Link Governor
- PSHE Lead
- ICT Curriculum Lead
- Subject Leaders
- ICT Technical Coordinator/Technician
- Data Protection Officer
- Volunteers and contractors (including tutor)
- Pupils
- Parents/carers
- External groups including parent associations

All staff

All staff should sign and follow the staff Acceptable Use Agreement in conjunction with this policy, the school's main Safeguarding Policy, the Code of Conduct/Staff Handbook and relevant parts of Keeping Children Safe in Education to support a whole-school safeguarding approach.

This includes:

- Report any concerns, no matter how small, to the Designated Safeguarding Lead, maintaining an awareness of current online safety issues and guidance (such as KCSIE), modelling safe, responsible and professional behaviours in their own use of technology at school and beyond and avoiding scaring, victim-blaming language.
- Staff should be aware of the new DfE standards and relevant changes to filtering and monitoring and play their part in feeding back about over-blocking, gaps in provision or pupils bypassing protections. All staff are also responsible for the physical monitoring of pupils' online devices during any session/class they are working within.

Headteacher

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding.
- Oversee and support the activities of the designated safeguarding lead team and ensure they work technical colleagues to complete an online safety audit in line with KCSIE, including technology in use in the school.
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnership support and guidance.
- Ensure ALL staff undergo safeguarding training (including online safety) at induction and with regular updates and that they agree and adhere to policies and procedures.

- Ensure ALL governors and trustees undergo safeguarding and child protection training and updates (including online safety) to provide strategic challenge and oversight into policy and practice and that the governors are regularly updated on the nature and effectiveness of the school's arrangements.
- 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 remote systems are implemented according to child-safety first principles.
- Better understand, review and drive the rationale behind decisions in filtering and monitoring as per the new DfE standards—through regular liaison with technical colleagues and the DSL– in particular understand what is blocked or allowed for whom, when, and how as per KCSIE.
- Liaise with the designated safeguarding lead / Online Safety Officer on all online safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- Support safeguarding leads and technical staff as they review protections for pupils in the home and remote-learning procedures, rules and safeguards.
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors 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.
- 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 the school website meets statutory requirements.

Designated Safeguarding Lead / Online Safety Officer

- The DSL should "take **lead responsibility** for safeguarding and child protection, **including online safety and understanding the filtering and monitoring** systems and processes in place.
- Ensure "An effective whole school approach to online safety as per KCSIE.
- Ensure the school is complying with the DfE's standards on Filtering and Monitoring.
- As part of this, DSLs will work with technical teams to carry out reviews and checks on filtering and monitoring, to compile the relevant documentation and ensure that safeguarding and technology work together. This will include a decision on relevant YouTube mode (currently unrestricted on Class teachers and Administrative Desktops) and preferred search engine/s (Kiddle and Swiggl for EYFS and KS1, MS edge for KS2 and staff).
- Where online-safety duties are delegated and in areas of the curriculum where the DSL is not directly responsible but which cover areas of online safety (e.g. PSHE), ensure there is regular review and open communication and that the DSL's clear overarching responsibility for online safety is not compromised or messaging to pupils confused.
- Ensure ALL staff and supply staff undergo safeguarding and child protection training (including online-safety) at induction and that this is regularly updated.
    - This must include filtering and monitoring and help them to understand their roles.
    - All staff must read KCSIE Part 1 and all those working with children also Annex B.
    - Cascade knowledge of risks and opportunities throughout the organisation.

- Ensure that ALL governors undergo safeguarding and child protection training (including online-safety) at induction to enable them to provide strategic challenge and oversight into policy and practice and that this is regularly updated.
- Take day-to-day responsibility for safeguarding issues and be aware of the potential for serious child protection concerns.
- Be mindful of using appropriate language and terminology around children when managing concerns, including avoiding victim-blaming language.
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply.
- Work closely with SLT, staff and technical colleagues to complete an online safety audit (including technology in use in the school).
- Work with the Headteacher, DPO and governors 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 carful and legal sharing of information.
- Stay up to date with the latest trends in online safeguarding and undertake Prevent awareness training.
- Review and update this policy, other online safety documents (e.g. Acceptable Use Agreements) and the strategy on which they are based, in harmony with policies for behaviour, safeguarding, Prevent and others, and submit for review to the governors.
- Receive regular updates in online safety issues and legislation - e.g. CEOP, School's National Online Safety subscription and be aware of local and school trends.
- Ensure that safety education is embedded across the curriculum in line with the PSHE guidance and beyond, in wider school life.
- Promote an awareness and commitment to online safety throughout the school community.
- Communicate regularly with SLT and the safeguarding Governor to discuss current issues, review incident and filtering logs. Discuss how filtering and monitoring work and have been functioning or helping.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident, and these are logged in the same way as any other safeguarding incident.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown.
- Ensure staff adopt a zero-tolerance, whole school approach to all forms of child-on-child abuse, and don't dismiss it as banter (including bullying).
- Pay particular attention to online tutors, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUA, and those hired by parents

Governing Body, led by Online Safety / Safeguarding Link Governor

- Approve this policy and review the effectiveness of the policy.
- Undergo, and signpost all other governors and Trustees to attend, safeguarding and child protection training including online safety at induction to provide strategic challenge and into policy and practice, ensuring this is regularly updated.
- Ensure that all staff also receive appropriate safeguarding and child protection (including online) training at induction and that this is updated.
- Appoint a filtering and monitoring governor to work closely with the DSL on the new filtering and monitoring standards.

- Support the school in encouraging parents and the wider community to become engaged in online safety activities.
- Have regular strategic reviews with DSL and incorporate online safety into standing discussions of safeguarding at governor meeting.
- Work with the DPO, DSL and Headteacher 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.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex B.
- Ensure that all staff undergo safeguarding and child protecting training (including online safety, filtering and monitoring).
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.

PSHE Lead

- As listed in the 'all staff' sections, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / Relationships education, relationships and sex education and health education curriculum. "This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. Throughout these subjects, teachers will address online safety and appropriate behaviour in an age appropriate way that is relevant to their pupils' lives.
- Focus on the underpinning knowledge and behaviours in an age appropriate way to help pupils to navigate the online world safely and confidently regardless of their device, platform or app.
- Access teaching to "identify where pupils need extra support or intervention through test, written assignments or self-evaluations, to capture progress" to complement the ICT curriculum.
- Work closely with the DSL/Online Safety Officer and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.
- Note that PSHE policy should be included on the school website.
- Work closely with the ICT subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach.

ICT Curriculum Lead

- As listed in the 'all staff' sections, plus:
- Oversee the delivery of the online safety element of the ICT curriculum.
- Work closely with the PSHE lead to avoid overlap but ensure a complementary whole-school approach.
- Work closely with the DSL/Online Safety Officer and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements.

Subject Leaders

- As listed in the 'all staff' sections, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike.

- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context.
- Work closely with the DSL/Online Safety Officer and all other staff to ensure an understanding of the issues, approaches and messaging within Computing.
- Ensure subject specific action plans also have an online safety element.

IT Technical Coordinator/Technician (working with the IT Managed Services Provider)

- As listed in the 'all staff' sections, plus:
- Collaborate regularly with the DSL and SLT to help them make key strategic decisions around the safeguarding elements of technology.
- Support safeguarding teams to understand and manage these systems and carry out regular reviews and annual checks.
- Support DSLs and SLT to carry out an annual online safety audit as recommended in KCSIE. This includes a review of technology, including filtering and monitoring systems (what is allowed, blocked and why and how 'over blocking' is avoided as per KCSIE) to support their role as per the DfE standards, protections for pupils in the home during remote-learning.
- Keep up to date with the school's Online Safety Policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- Work closely with the DSL / Online Safety Officer/ DPO / PSHE lead to ensure that school systems and networks reflect school policy and there are no conflicts between educational messages and practice.
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems; especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.
- Ensure filtering and monitoring systems work on new devices and services before releasing them to pupils and staff.
- Maintain up-to-date documentation of the school's online security and technical procedures.
- To report online safety related issues come to their attention in line with school policy.
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Ensure the Privacy policy are up to date, easy to follow and practicable.
- Monitor the use of school technology, online platforms and social media presence. Any misuse and/or attempted misuse is reported to the Online Safety Officer.
- Work with the Headteacher to ensure the school website meets statutory DfE requirement.

Data Protection Officer (DPO)

- Alongside those of other staff, provide data protection expertise and training and support the DP and compliance with those and legislation and ensure that the policies conform with each other and with this policy.
- Not prevent, or limit, the sharing of information for the purposes of keeping children safe. As outlined in Data protection in schools, 2023, "It's not usually necessary to ask for consent to share personal information for the purposes of safeguarding a child." And in KCSIE 2023, "The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to

stand in the way of the need to safeguard and promote the welfare and protect the safety of children."

- Note that retention schedules for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

Volunteers and contractors (including tutor)

- Read, understand, sign and adhere to an acceptable use agreement (AUA).
- Report any concerns, no matter how small, to the DSL / Online Safety Officer
- Maintain an awareness of current online safety issues and guidance.
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications.
- Note that as per Acceptable Use Agreement contractor will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

- Read, understand and sign with their parents and adhere to the Acceptable Use Agreement – Parents and Pupils.

Parents/Carers

- Read, sign and adhere the school's Parental Acceptable Use Agreement, read the pupil AUA and encourage their children to follow it.

External groups including Parent groups

- Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology or the internet within school.
- Support the school in promoting online safety and data protection
- 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, governors, contractors, pupils or other parents/carers.

Appendix 2 – Staff, Governors and Volunteers Acceptable Use Agreement

Oakhyrst Grange School is committed to safeguarding and promoting the welfare of children and young people and expects all staff (including support and peripatetic staff), governors and volunteers to share this commitment. At this school we respect and value all children and are committed to providing a caring, friendly and safe environment for our pupils so that they can learn in a relaxed and secure atmosphere. We believe that every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Oakhyrst Grange School. We recognise our responsibility to safeguard all who access our school and to promote the welfare of all of our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

We ask everyone involved in the life of Oakhyrst Grange School to sign an Acceptable Use Agreement (AUA), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media both when on school site and outside of school.

Acceptable Use Agreement

This AUA is reviewed annually, and staff, governors and volunteers are asked to sign it when starting at the school and whenever changes are made. All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

We asked everyone involved in the life of Oakhyrst Grange School are to sign an Acceptable Use Agreement which outlines how the school expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

If you have any questions about this AUA or our approach to online safety, please speak the Online Safety Officer.

What I am agreeing to?

1. For Staff and governors:
   I have read and understood Oakhyrst Grange School's full Online Safety Policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviours as an adult and enforcing the rules for pupils. I will report any breaches or suspicions, by adults or children, in line with the policy without delay as outlined in the Online Safety Policy.
2. I understand online safety is a core part of safeguarding and part of everyone's job. It is my duty to support a whole-school safeguarding approach and to learn more each year about best-practice in this area. I have noted the section in our Online Safety Policy which describes trends over the past year at a national level and/or at this school.
3. I will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher/Principal (if by an adult) and make them aware of new trends and patterns that I might identify.
4. I will follow the guidance in the Safeguarding Policy and Online Safety Policy for reporting incidents (including for handling incidents and concerns about a child in general, sharing nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, misuse of technology and social media).

5. I understand the principle of 'safeguarding as a jigsaw' where my concern or professional curiosity might complete the picture. Online-safety issues (particularly relating to bullying and sexual harassment and violence) are most likely to be overheard in the playground, corridors, toilets and other communal areas outside the classroom.
6. I will take zero tolerance approach to all forms of child-on-child abuse (not dismissing it as banter), including bullying, sexual violence and harassment and maintains an attitude of 'it could happen here'.
7. I will be mindful of using appropriate language and terminology around children when addressing concerns, including avoiding victim-blaming language.
8. I will identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the PSHE curriculum, 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).
9. When overseeing the use of technology in school or for homework or remote teaching, I will encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place and how they keep children safe).
10. I will check with the Online Safety Officer if I want to use any new platform of app that has not already been approved by the school, to ensure this is quality assured.
11. I will follow best-practice pedagogy for online safety education, avoiding scaring and other unhelpful prevention methods.
12. I will prepare and check all online and classroom resources **before** using them, for accuracy and appropriateness (including ensuring adverts do not play at the beginning of videos). I will flag any concerns about "overblocking" to the DSL such as if I cannot access teaching materials.
13. I will carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age-appropriate materials and signposting, and legal issues such as copyright and data protection.
14. I will physically monitor pupils using online devices in the classroom to ensure appropriate and safe use.
15. I will leave my phone, or other capture device, in my cabinet or drawer (locked if possible) and muted. Under no circumstances will I use it in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the Headteacher and it will be done in the presence of a member staff. The same principles apply for wearable technology. Smart glasses should not be worn in school.
16. During any periods of remote learning, I will not behave any differently towards pupils compared to when I am in school and will follow the same safeguarding principles as outlined in the main Child Protection and Safeguarding Policy when it comes to behaviour, ways to contact and the relevant systems and behaviours.
17. I understand that school systems and users are protected by security, monitoring and filtering services, and that my use of school devices, systems and logins on my own devices and at home (regardless of time, location or connection), including encrypted content, may be monitored/captured/viewed by the relevant authorised staff members.
18. I know the filtering and monitoring systems used within school and the types of content blocked and am aware of the increased focus on these areas in KCSIE. If I discover pupils may be bypassing blocks or accessing inappropriate material, I will report this to the DSL without delay. Equally, if I feel that we are overblocking, I shall notify the school to inform regular checks and annual review of these systems.

19. I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology both in and outside school, including on social media, e.g. by not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
20. I will NOT contact or attempt to contact any pupil or to access their contact details (including their usernames/handles on different platforms) in any way other than school-approved and school-monitored ways, which are detailed in the school's Online Safety Policy. I will report any breach of this by others or attempts by pupils to do the same to the Headteacher.
21. If I already have a personal relationship to a pupil or their family, I will inform the DSL/Headteacher of this as soon as possible.
22. I will NOT use any new technology or download any apps without agreement from the DSL/Online Safety Officer.
23. I will NEVER use a mobile hotspot to provide internet to any device that belongs to the school.
24. I will NEVER use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.
25. I will NOT support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.
26. I will ONLY use gen AI platforms that have been authorised for use, including those used with pupils and to support administrative tasks, and I will ensure that any use of these platforms is transparent, appropriate, legal and ethical. I will also ensure that I abide by all data protection legislation in relation to using these platforms.
27. I understand that breach of this AUA and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

To be completed by the user

I have read, understood and agreed to this policy. I understand that it is my responsibility to ensure I remain up to date and read and understand the school's most recent online safety / safeguarding policies. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: ____

Name: ____

Role: ____

Date: ____

Appendix 2a -Request to use personal mobile device in school (e.g Medical)

Name:	
Job Title:	
Mobile device (make and model):	
Wi-Fi ONLY device:	Yes / No
If not, please specify mobile device number:	
Duration I will be using my own device: DD/MM/YYYY	From: To: 31/08/
Reason(s) for using personal device: Please include name(s) of software and/or applications	
Any pupil's information kept on the device (e.g. personal information, statistics, photos, audio, video etc.) All pupil information must be retained only until the end of the school day. Under no circumstances should pupil data be stored or transferred to personal devices or taken off school premises.	Yes / No

I have read and understand the Staff AUA and the school's full Online Safety Policy. I will only use my personal device for the reason(s) stated above and I fully understand that I am ultimately responsible for my own actions.

Signature: _________________________________ Date: ______________________

Approved by:

Signature: _________________________________Date: _______________________

Name and title: ____(printed)

Appendix 2b -Request for installation of software in School device(s)

Name:	
Job Title:	
Software	
Name:	
Operation System (Windows/iOS/Chrome):	
Company:	
Version:	
Price (Approx.):	
Location of the software to be installed: (Please provide PC tag number if appropriate)	
If the software uses pupil's information, please confirm the software and any cloud-based storage is UK GDPR and Data protection compliance	Yes / No
Period I will be using the software: DD/MM/YYYY	From: To:
Reason for request:	

I have read and understand the Staff AUA and the school's full Online Safety Policy. I will only use the software above for the reason(s) stated above and I fully understand that I am ultimately responsible for my own actions.

Signature: _________________________________ Date: ______________________

Approved by:

Signature: _________________________________Date: _______________________

Name and title: ____(printed)

Appendix 2c – Request for Remote Access (VPN)

Section 1 – Applicant Information

- Full Name: ____________________________
- Job Title / Department: ____________________________
- Employee / Contractor ID: ____________________________
- Email Address: ____________________________
- Contact Number: ____________________________

Section 2 – Access Details

- **Reason for VPN Access from Home**
  ☐ Remote Work and
  ☐ Access to Network Resources
  ☐ System Administration
  ☐ Other: ____________________________
- **Duration of Access Needed:**
  ☐ Temporary (From: _____________ To: ____________)
  ☐ Ongoing

Section 3 – Laptop Details

- Device Make & Model: ____
- Operating System & Version: ____
- Antivirus: ___________________________________ ☐ Yes ☐ No
- Firewall: ____________________________________☐ Yes ☐ No
- Encryption Enabled: ☐ Yes ☐ No

Section 4 – Security Compliance and acknowledgement

By signing below,
For Personal Laptops, I confirm that:

1. My personal laptop meets the organisation's security requirements.
2. I will not store sensitive company data locally unless encrypted.
3. I understand that VPN access may be revoked at any time for non-compliance.
4. The school will install the necessary VPN software on my personal laptop. However, the school **cannot assume responsibility and is not liable** for any potential device issues, data loss, or performance impacts resulting from the installation.

I acknowledge that:

1. VPN access is for authorised school-related work purposes only.
2. I will report any security incidents immediately.
3. I will not share my credentials with anyone.
4. I understand that all VPN activity may be monitored for security purposes.

Applicant Signature: ____ Date: __________

Section 5 – Approval

Headteacher Approval: ☐ Approved ☐ Denied

Name & Signature: ____ Date: __________

IT Security Approval: ☐ Approved ☐ Denied

Name & Signature: ____ Date: __________

Appendix 3: Acceptable Use Agreement – Parents and Pupils

Oakhyrst Grange School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. At this school we respect and value all children and are committed to providing a caring, friendly and safe environment for our pupils so that they can learn in a relaxed and secure atmosphere. We believe that every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Oakhyrst Grange School. We recognise our responsibility to safeguard all who access our school and to promote the welfare of all of our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

Oakhyrst Grange School provides access to networked computers to support pupil's academic work. Our Acceptable Use Agreement is an extension to the behaviour guidelines. It includes guidelines for the safe and responsible use of the network and the Internet as well as school online platforms that include but are not limited to Tapestry, Seesaw, Zoom, Teams and any other app or website that the children or parents access to communicate with staff or access work set by teachers. It also identifies activities that constitute an abuse of our ICT facilities. This agreement is reviewed annually. Please refer to our full Online Safety Policy which is available on the School Website for your inspection.

Acceptable Use Agreement – Parents

The use of technology is an essential part of all of our lives. At Oakhyrst Grange school take our responsibilities for supporting your child to develop skills in using technology very seriously, and their safety and wellbeing are our utmost priority to us.

We ask all children, young people and adults involved in the life of Oakhyrst Grange school to read and sign an Acceptable Use Agreement (AUA) to outline how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

We tell your children that **they should not behave any differently when they are out of school or using their own device or on a home network.** What we tell pupils about behaviour and respect applies to all members of the school community, whether they are at home or school. We seek the support of parents and carers to reinforce this message and help children to behave in a safe way when online:

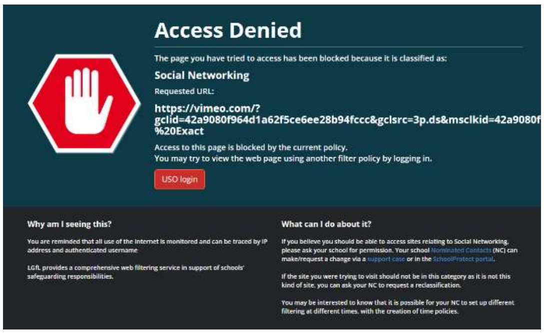
"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

Please read our Online Safety Policy for more detail on our approach to online safety and links to other relevant policies such as Safeguarding and Child Protection Policy, Behaviour Policy etc. If you have any questions about this AUA or our approach to online safety, please speak to our Online Safety Officer.

What I am agreeing to?

1. I understand that Oakhyrst Grange School uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the smooth running of the school, and to help prepare the children and young people in our care for their future lives.

2. I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate material, including behaviour policies and agreements, physical and technical monitoring, education and support and web filtering.
3. School network protections will be superior to most home filtering. However, please note that accessing the internet always involves an element of risk and the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies. Schools are asked not to overblock or provide an experience which is so locked down as to block educational content or not train pupils for life in an online world.
   Example of website content blocked:



Access Denied

The page you have tried to access has been blocked because it is classified as:

Social Networking

Requested URL:

https://vimeo.com/?gclid=42a9080f964d1a62f5ce6ee28b94fccc&gclsrc=3p.ds&msclkid=42a9080f%20Exact

Access to this page is blocked by the current policy.
You may try to view the web page using another filter policy by logging in.

Why am I seeing this?

You are reminded that all use of the internet is monitored and can be traced by IP address and authenticated username

LGfL provides a comprehensive web filtering service in support of schools' safeguarding responsibilities.

What can I do about it?

If you believe you should be able to access sites relating to Social Networking, please ask your school for permission. Your school Nominated Contacts (NC) can make/request a change via a support case or in the SchoolProtect portal.

If the site you were trying to visit should not be in this category as it is not this kind of site, you can ask your NC to request a reclassification.

You may be interested to know that it is possible for your NC to set up different filtering at different times, with the creation of time policies.

4. I understand that internet and device use in school, and use of school-owned devices, networks and cloud platforms out of school may be subject to filtering and monitoring.
5. I understand and will help my child to use any devices at home in the same manner as when in school, including during any remote learning periods.
6. I will support my child to follow the school's policy regarding bringing devices to school. Pupils are not allowed mobile devices including smart watches etc. in school. See Online Safety Policy /Social Media/Device Usage/Pupils section for exceptions.
7. For parents with children in Coding Club, please read the Scratch Online information sent home especially regarding Comments/likes/share projects.
8. I understand that my child might be contacted online on and only about their learning, wellbeing or behaviour. If they are contacted by someone else or these staff ask them to use a different app to chat, please report this to the Headteacher.
9. I will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including on social media, not sharing other's images or details without permission and refraining from posting negative, threatening comments about others including the school staff, volunteers, governors, pupils or other parent/carer(s).
10. The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's Online Safety Policy and not encourage my child to join any platform where they are below the minimum age (for nearly every social media platform, this means under 13).
11. When I visit the school premises, I will keep any online technology in my pocket wherever possible.
12. I will follow the school's Online Safety Policy, which outlines when I can capture and/or share images/videos. I will **not** share images of other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous. The school sometimes uses images/video of my child for internal purposes such as recording attainment, but it will only do so publicly if I have given my consent. I will not share images of

other people's children on social media and understand that there may be cultural or legal reasons why this would be inappropriate or even dangerous.

13. I will not covertly film or make recordings of any interactions with pupils or adults in schools. If I wish to make any recording, we request you to please speak to the Headteacher.
14. I understand that for my child to grow up safe online, she/he will need positive input from school and home. I will talk to my child about online safety and either speak to school or refer to the schools subscribed The National College website or parentsafe.lgfl.net for advice and support on safe settings, parental controls, apps and games, talking to them about life online, screen time and relevant topics from bullying to accessing pornography, extremism and gangs, sharing inappropriate content etc.
15. Research tells us that the majority of children are now accessing artificial intelligence in some form, which is available for free on most mainstream apps and social media platforms. There are some significant risks involved with this including talking to chatbots, and the use of nudifying apps and image creators to create inappropriate and illegal images/videos I will talk to my child about these risks. You can find out more at parentsafe.lgfl.net
16. I understand that my child needs a safe and appropriate place for home learning whether for homework or during times of school closure. When on any video calls with school, my child will be fully dressed and not in bed, and the camera angle will point away from bed, bedding, personal information etc. Where it is possible to blur or change the background, I will help my child to do so.
17. If my child has online tuition, I will refer to the Online Tutors – Keeping children Safe poster and undertake necessary checks where I have arranged this privately, ensuring they are registered, safe and reliable, and for any tuition to remain in the room where possible, ensuring my child knows that tutors should not arrange new sessions or online chats directly with them.
18. I understand that whilst home networks are much less secure than school ones, I can apply child safety settings to my home internet. Internet Matters (internetmatters.org) provides guides to help parents do this easily for all the main internet service providers in the UK.
19. There are also child-safe search engines e.g. swiggle.org.uk and YouTube Kids is an alternative to YouTube with age appropriate content.
20. I understand that it can be hard to stop using technology sometimes, and I will talk about this to my children, and refer to the principles of the Digital 5 A Day by Children's Commissioner for England https://www.childrenscommissioner.gov.uk/
21. I will not attempt to track my child during the school day or on school trips, e.g. with Apple AirTags or similar devices. Not only is this against the terms and conditions of these products, it is unhelpful to the operation of the school, can broadcast the location of children to passing users and can lead to unnecessary distress among parents e.g. if a school trip has an unannounced change of route or schedule.
22. There are other organisations and sites which support parents:
    - London Grid for learning https://parentsafe.lgfl.net/
    - The National College https://nationalcollege.com/
    - NSPCC https://www.nspcc.org.uk,
    - CEOP Education http://www.thinkuknow.co.uk
23. I understand and support the commitments made by my child in the Acceptable Use Agreement, which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

24. I can find out I can find out more about online safety at Oakhyrst Grange School by reading the Online Safety Policy and can talk to the school if I have any concerns about my child/ren's use of technology, or about that of others in the community, or if I have questions about online safety or technology use in school.

I/We have read, understood and agreed to this agreement.

Signature/s: ____

Name/s of parent / guardian: ____

Parent / guardian of: ____

Date: ____

Oakhyrst Grange School

Acceptable Use Agreement – EYFS Pupils

My name is ____________________

1. I only **USE** devices or apps, sites or games if a trusted adult says so □
2. I **ASK** for help if I'm stuck or not sure; I **TELL** a trusted adult if I'm upset, worried, scared, uncomfortable or confused □
3. I look out for my **FRIENDS** and tell someone if they need help □
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult □
5. I **KNOW** people online aren't always who they say they are and things I read are not always **TRUE** □
6. Anything I do online can be shared and might stay online **FOREVER** □
7. I don't keep **SECRETS** 🚫 unless they are a present or nice surprise □
8. I don't have to do **DARES OR CHALLENGES** ❌, even if someone tells me I must. □
9. I don't change **CLOTHES** or get undressed in front of a camera □
10. I always check before **SHARING** personal information or other people's stories and photos □
11. I am **KIND** and polite to everyone □

My trusted adults are:

____ at school

____ at home

We understand that your child is too young to give informed consent on his/her own; however, we feel it is good practice to involve them as much as possible in the decision-making process, and believe a shared commitment is the most successful way to achieve this.

I have read and understood the Online Safety Policy and give permission for my child to access the Internet at school, and will encourage them to abide by the above rules**.**

Signature/s: ____

Name/s of parent / guardian: ____

Parent / guardian of: ____

Date: ______________________________________

Acceptable Use Agreement – Pupils

- ***I learn online*** - I use the school's internet, devices and logins for schoolwork, homework and other activities e.g. play educational games and research topics. School can see what I am doing to keep me safe, even when at home.
- ***I behave the same way on devices as face to face in the classroom, and so do my teachers*** – If I get asked to do anything that I would find strange in school, I will tell another teacher.
- ***I ask permission*** - At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
- ***I am a good friend online*** – I won't share or message or say anything I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
- ***I am creative online*** – I don't just use apps, sites and games to look at things other people made or posted; I also get creative to learn or make things.
- ***I am not a bully*** – I know just calling something fun or banter doesn't stop it hurting someone else. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
- ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
- ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
- ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything I see or read upsets, worries or makes me feel uncomfortable on an app, site or game. If I get a funny feeling, I talk about it.
- ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult.
- ***If I make a mistake I don't try to hide it but ask for help.***
- ***I communicate and collaborate online*** - with people I already know and have met in real life or that a trusted adult knows about.
- ***I know online friends might not be who they say they*** are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
- ***I never pretend to be someone else online*** – it can be upsetting or even dangerous.
- ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
- ***I don't go live (videos anyone can see) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
- ***I don't take photos or videos or people without them knowing or agreeing to it*** – and I never film fights or people when they are upset or angry. Instead ask an adult or help if it's safe.
- ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

- ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
- ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
- ***I follow age rules*** – 13+ games, apps and films aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
- ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
- ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
- ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
- ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
- ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
- ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, and I know which sites to trust, and how to double check information I come across. If I am not sure I ask a trusted adult.

I have read and understood this agreement. If I have any questions, I will speak to a trusted adult:

At school that might mean ____

Outside school, my trusted adults are___________________________________

Signed: ________________________ Date: ____________________

Appendix 4: Acceptable Use Agreement – Visitors and Contractors

Oakhyrst Grange School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment. At this school we respect and value all children and are committed to providing a caring, friendly and safe environment for our pupils so that they can learn in a relaxed and secure atmosphere. We believe that every pupil should be able to participate in all school activities in an enjoyable and safe environment and be protected from harm. This is the responsibility of every adult employed by, or invited to deliver services at Oakhyrst Grange School. We recognise our responsibility to safeguard all who access our school and to promote the welfare of all of our pupils by protecting them from physical, sexual and emotional abuse, neglect and bullying.

Visitors and contractors are asked to sign this document before they are allowed access to the school or its pupils. Many of these rules are common sense – if you are in any doubt or have questions, please ask the DSL. If you have any questions during your visit, you must ask the person accompanying you. If questions arise after your visit, please email or call the school office.

Please refer to our full Online Safety Policy which is available on the School Website for your inspection.

Acceptable Use Agreement – Visitors and Contractors

- I understand that any activity on a school device or using school networks, platforms, internet and logins may be captured by one of the school's security, monitoring and filtering systems and/or viewed by an appropriate member of staff.
- I will never attempt to arrange any meeting with a pupil, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- I will leave my phone in my pocket and muted. Under no circumstances will I use it (or other capture device) in the presence of children or to take photographs or audio/visual recordings of the school, its site, staff or pupils. If required (e.g. to take photos of equipment or buildings), I will have the prior permission of the headteacher (this may be delegated to other staff) and it will be done in the presence of a member staff. The same principles apply for wearable technology. Smart glasses should not be worn in school. Please speak to the Headteacher if this presents any issue.
- If I am given access to school-owned devices, networks, cloud platforms or other technology:
  - I will use them exclusively for the purposes to which they have been assigned to me, and not for any personal use
  - I will not attempt to access any pupil / staff / general school data unless expressly instructed/allowed to do so as part of my role
  - I will not attempt to contact any pupils or to gain their contact details under any circumstances
  - I will protect (and not share) my username/password and notify the school of concerns.
  - I will abide by the terms of the school Data Privacy Policy protections
  - I understand that my online activity will be subject to the school's filtering and monitoring systems, and that any attempts to access content which is illegal or inappropriate for a school setting, may result in further action as per the safeguarding procedures and may result in termination of contract.

- I will not share any information about the school or members of its community that I gain as a result of my visit in any way or on any platform except where relevant to the purpose of my visit and agreed in advance with the school.
- I will not reveal any information on social media or in private which shows the school in a bad light or could be perceived to do so.
- I will not do or say anything to undermine the positive online safety messages that the school disseminates to pupils and will not give any advice on online safety issues unless this is the purpose of my visit and this is pre-agreed by the school. NB – if this is the case, the school will ask me to complete Annex A and consider Annex B of 'Using External Visitors to Support Online Safety' from the UK Council for Child Internet Safety (UKCIS).
- I understand that children can be abused and harmed when using devices and I will report any behaviour (no matter how small) which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a child) or Headteacher (if by an adult)
- I will only use any technology during my visit, whether provided by the school or my personal/work devices, including offline or using mobile data, for professional purposes and/or those linked to my visit and agreed in advance. I will not view any content or material which is or could be perceived to be inappropriate for children or an educational setting. I will not use a mobile hotspot to provide internet to any device I use in school.
- If I need to use any specific applications, I must seek authorisation from the Headteacher before doing so. In particular this includes AI.
- I will behave in a professional and responsible manner at all times and understand that failure to do so may result in further action being taken and could result in the termination of my contract.

To be completed by the visitor/contractor:

I have read, understood and agreed to this policy.

Signature/s: ____

Name: ____

Organisation: ____

Visiting / accompanied by: ____

Date / time: ____

To be completed by the school (only when exceptions apply):

Exceptions to the above policy: ____

Name / role / date / time: ____

Appendix 5: Remote Access Agreement

Purpose

This agreement outlines the terms and conditions for authorised employees, contractors, or partners to access the Oakhyrst Grange School's internal network via a Virtual Private Network (VPN). The goal is to ensure secure, compliant, and responsible use of remote access resources, minimising risks associated with unauthorised use or malicious attack that could result in:

- Loss of sensitive or confidential data
- Loss of intellectual property
- Damage to the school's reputation
- Damage to critical internal systems
- Financial penalties or liabilities

Context

Until recently, Oakhyrst Grange school systems were inaccessible from outside the school premises. Implementing remote access provides several benefits, including:

- What can be accessed e.g. resources available to a staff member
- Where it can be accessed e.g. from home
- When it can be accessed e.g. outside school hours

Scope

This agreement applies to all individuals granted VPN access to the school's systems, data, and application using either school-owned or authorised personal devices to access school data and networks remotely. Remote access privileges are not automatically granted and require approval.

Security Requirements

- Devices must have up-to-date antivirus, firewall, and operating system patches.
- Multi-factor authentication (MFA) must be enabled for VPN login.
- Authorised Users (AUs) must not share VPN credentials with anyone.
- All data transmitted must be encrypted.

Connection Procedures

Technology

All remote access connections will be centrally managed by the IT department using encryption and strong password protection with multi-factor authentication. Remote access is permitted ONLY via the LGfL Cisco VPN client, provided by IT department.

System Requirements

Staff using personal devices must ensure:

- Windows 11 with the latest updates installed
- Up-to-date antivirus software
- Active internet connection

Monitoring & Compliance

Oakhyrst Grange School reserves the right to monitor VPN usage for security and compliance purposes. Any violation of this agreement may result in disciplinary action, up to and including termination of access or employment.

User Responsibilities

- AUs must treat remote access connections with the same level of security as on-site connections.
- Disconnect/Log out of the VPN when not actively working.

- When using personal devices, AUs must prevent access by non-authorised individuals.
- Report any suspected security incident immediately to IT Department.
- Refer to the Acceptable Use Policy for further details.

Prohibited Activities

- Connecting to the VPN from unsecured public Wi-Fi.
- Connect to other networks simultaneously (except for internet access)
- Unauthorised access to systems, data, or applications.
- Downloading or storing sensitive data on personal devices without explicit approval.
- Circumventing security controls or monitoring tools.

To be completed by the user

I have read, understood and agreed to this agreement. I understand that failure to comply with this agreement could lead to disciplinary action.

Signature: ____

Name: ____

Role: ____

Date: ____