Windlesham School & Nursery

Online Safety Policy

Last Reviewed: October 2025

Next Review Due: October 2026

Reviewed by:

Nick Matthews : Headteacher & DSL

Jack Cornish, Co-Chair of Governors (Safeguarding)

Windlesham School & Nursery

INDEPENDENT SCHOOLS ASSOCIATION Accredited Member

Table of Contents

Appendices

1. Introduction

Key people & dates

Windlesham School	Designated Safeguarding Lead (DSL)	Mr Nick Matthews
	Online-safety & safeguarding link governor	Mr Jack Cornish
	PSHE/RHSE lead	Ms Dorricott Juniper
	Network manager	Mike Bush – Virtual IT Education
	Computing Lead	Mme Flynn
	Data Protection Officer	Samantha Roberts

1. What is the policy?

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' Sept 2025, 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2025 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, and Computing; it is designed to sit alongside the school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures found on the school's website.

Who is it for; when is it reviewed?

This policy should be a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and statutory regulations, Windlesham School aims to involve staff, governors in writing and reviewing the policy. This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Acceptable Use Policies (see appendices) are reviewed alongside this overarching policy. Any changes to this policy will be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

Windlesham School's named online-safety lead is the designated safeguarding lead (DSL). KCSIE makes clear that "the designated safeguarding lead should take **lead** responsibility for safeguarding and child protection (including online safety)." The DSL (who is also the head) will collaborate with the Computing Lead, the external IT support agencies and the staff body.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 4 C's: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2025, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design.

In past and potential future **remote learning and lockdowns**, there is a greater risk for grooming and exploitation (CSE, CCE and radicalisation) as children spend more time at home and on devices. There is a real risk that some pupils may miss opportunities to disclose such abuse during any periods of remote learning.

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff Team/Sharepoint
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)

- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school and annually, in January each year.
- Reviews of this online-safety policy will include input from staff and other stakeholders, helping to ensure further engagement

Overview

2. Aims

This policy aims to:

- Set out our expectations for all Windlesham community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online and 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
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of todays and tomorrow's digital world.
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
    - for the protection and benefit of the children and young people in their care, and
    - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
    - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with our Safeguarding Policy. The DSL will handle referrals to Front Door for Families (FDFF) in Brighton and Hove and normally the Headteacher or the DSL will handle referrals to the Local Authority Designated Officer (LADO). Beyond this, Windlesham has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the NSPCC Whistleblowing Helpline.

3. Scope

This policy applies to all members of the Windlesham community (including teaching and support staff, supply teachers, governors, volunteers, contractors, pupils, parents and carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

3 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.

Headteacher – Mr Nick Matthews

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Take overall responsibility (but not immediate oversight) for data management and information security ensuring the school's provision follows best practice in information handling; work with the Data Protection Officer (DPO) and governors to ensure a UK Data Protection Act 2018 -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
- Ensure the school implements and makes effective use of appropriate IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles (Annual safeguarding review, staff PDP meetings, weekly briefings)
- 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 that there is a system in place to monitor and support staff (e.g. network manager) who can carry out internal technical online-safety procedures
- Ensure governors are updated periodically on the nature and effectiveness of the school's arrangements for online safety
- Ensure the school website meets statutory requirements
- Developing the schools strategy on AI in conjunction with SLT and subject leader.

Designated Safeguarding Lead & Online Safety Lead – Mr Nick Matthews

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2025)

- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, IT support and SENDCOs) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- 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
- UK Data Protection Act 2018 is always put first, and data-protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safeguarding and "undertake Prevent awareness training." using the gov.uk resources.
- review and update this policy, other online safety documents annually (e.g., Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees. Use an appropriate audit tool to facilitate the review process eg LGFL Online Safety audit tool
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter

- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g., by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community.
- Communicate regularly with SLT and the designated safeguarding and online safety governor (Mr Jack Cornish) to discuss current issues (anonymised), review incident logs and filtering control logs and discuss how filtering and monitoring work and have been functioning.
- Monitor the use of school technology, online platforms and social media presence and that any misuse or attempted misuse is identified and reported in line with school policy.
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident.
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A. Ensure appropriate filters and appropriate monitoring systems are in place (see Pg. 19-20) be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when working remotely while in isolation/quarantine/lockdown, e.g., making an entry on the schools Engage portal.
- Oversee and discuss 'appropriate filtering and monitoring' with governors and ensure staff are aware. Windlesham's filtering system is Quantum, provided and managed by our network manager Virtual IT. The school's monitoring system is Smoothwall Ensure the is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.

Governing Body, led by Online Safety & Safeguarding Link Governor – Mr Jack Cornish

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2020)

- Approve this policy and strategy and subsequently review its effectiveness, e.g., by asking the questions in the helpful document from the UK Council for Child Internet Safety (UKCIS) Online safety in schools and colleges: Questions from the Governing Board
- Ask about how the school has reviewed protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- "Ensure an appropriate **senior member** of staff, from the school **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities

- Have regular strategic reviews with the DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and Headteacher to ensure a UK Data Protection Act 2018 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 Governors have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A. Ensure appropriate filters and appropriate monitoring systems are in place (see Pg. 19-20) be careful that 'over-blocking' does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Ensure that children are taught about safeguarding, including online safety as part of providing a broad and balanced curriculum.
- Ensure that the headteacher has delivered staff safeguarding and child protection training at least annually (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated (as and when necessary). Induction and training should be in line with any advice from local safeguarding partners.

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) is – Mr N Matthews
- Read Part 1, Annex A and Annex B of Keeping Children Safe in Education 2025, whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and staff handbook.
- Be fully aware of the school's policy on the use of mobile phones and external devices
- Notify the DSL if policy does not reflect practice in school and follow escalation procedures if concerns are not promptly acted upon

- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE 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)
- Whenever overseeing the use of technology in school or for homework or remote teaching, 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)
- If supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the **20 Safeguarding Principles for Remote Lessons** infographic which applies to all online learning, also in Annex 7 of the Windlesham's Safeguarding Policy.
- 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 UK Data Protection Act 2018.
- Be aware of security best-practice at all times, including password hygiene and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions.
- Notify the DSL of new trends and issues before they become a problem
- Carefully consider the use of AI in the classroom and the risks associated to them. Where using AI ensure that it is closely monitoroied, has educational value and is not just generative AI to complete work.
- Take a zero-tolerance approach to bullying and low-level sexual harassment
- Be aware that you are often likely to see or overhear online-safety issues in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL know
- Receive regular updates from the DSL and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff. More guidance on this point can be found in this Online Reputation guidance for schools.
- All staff should attend appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

PSHE & RHSE Lead – Miss Dorricott-Juniper

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE and Relationships education, relationships and sex education (RSE) 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."
- This will complement the computing curriculum, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face. This includes how to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.
- Ensure that an up to date RSHE policy is included on the school website.
- Work closely with the Computing lead to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead – Mme Flynn

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum
- Ensure an up-to-date overview of the online safety aspect of the Computing curriculum is available to all year groups
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new 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 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

Network Manager – Mike Bush - Virtual IT Education

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT/DSL team as they review protections for pupils in the home and remote-learning procedures, rules and safeguards
- 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
- Meet the RSHE lead to see how the online-safety curriculum delivered through this subject can complement the school IT system and vice versa and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead, the data protection officer to ensure that school systems and networks reflect school policy
- Ensure the above stakeholders understand the consequences of existing services and of any changes to these systems
- Support and advise on the implementation of 'appropriate filtering and monitoring' as decided by the DSL and senior leadership team
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that 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
- Work with the Headteacher to ensure the school website meets statutory DfE requirements
- Assist the School to ensure they have the appropriate level of security protection procedures in place in order to safeguard the systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. In addition, Virtual IT Education will continue to strive to meet the Cyber security standards for schools and colleges.GOV.UK. Broader guidance on cyber security including considerations for governors and trustees can be found at Cyber security training for school staff - NCSC.GOV.UK.

Data Protection Officer (DPO) – Mrs Roberts

Key responsibilities:

- Liaise with Virtual IT Education to oversee smooth IT support in school

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "Data Protection legislation does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent or carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long-term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for all pupil records.

• Work with the DSL/Headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited.

- Work with the DSL/Headteacher, governors and the network managers, to ensure that the Cyber Security Standards are complied with. A copy of the standards and the measures undertaken to comply with these is available in Appendix 8.

Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP) (Appendix 3)
- Report any concerns, no matter how small, to the designated safety lead as named in the AUP
- 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 AUP agreement, a 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 or direct communication with a pupil.

Pupils

Key responsibilities: (also found in the IT curriculum overview)

- Read, understand, sign and adhere to the pupil acceptable use policy and review this annually (Appendix 4)
- Avoid any private communication or use of personal logins or systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices and logins used at home should be used just like if they were in full view of a teacher.
- Understand the benefits and opportunities and risks of the online world and know who to talk to at school or outside school if there are problems

Parents and carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) annually and read the pupil AUP and encourage their children to follow it and ensure they sign it
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Provide a safe network, with suitable age appropriate filters, to help ensure children are safe when surfing the internet at home.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

External groups including parent associations – Friends of Windlesham

Key responsibilities:

- Any external individual and or organisation will sign an acceptable use policy prior to using technology or the internet within school this will be via the signing process at front desk.
- Support the school in promoting online safety and data protection

- Model safe, responsible, respectful 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 and carers

4. Education and curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing/IT

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum stages and subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, 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 websites.

Equally, 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, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Windlesham, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety).

Annual reviews of curriculum plans (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

5. Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding, as well as being a curriculum strand of Computing, RSHE and Citizenship.

General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the designated safeguarding lead 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.

School procedures for dealing with online-safety will be addressed in this policy but may also impact on:

- Safeguarding and Child Protection Policy
- Anti-Bullying Pol
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies
- Prevent Risk Assessment
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

Windlesham commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school and that those from outside school will continue to impact on pupils when they come into school or during extended periods away from 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 designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. This should be done using MyConcern and contact made with the DSL personally.

Any concern or allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors governors@windleshamschool.co.uk and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline on 0800 800 5000.

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

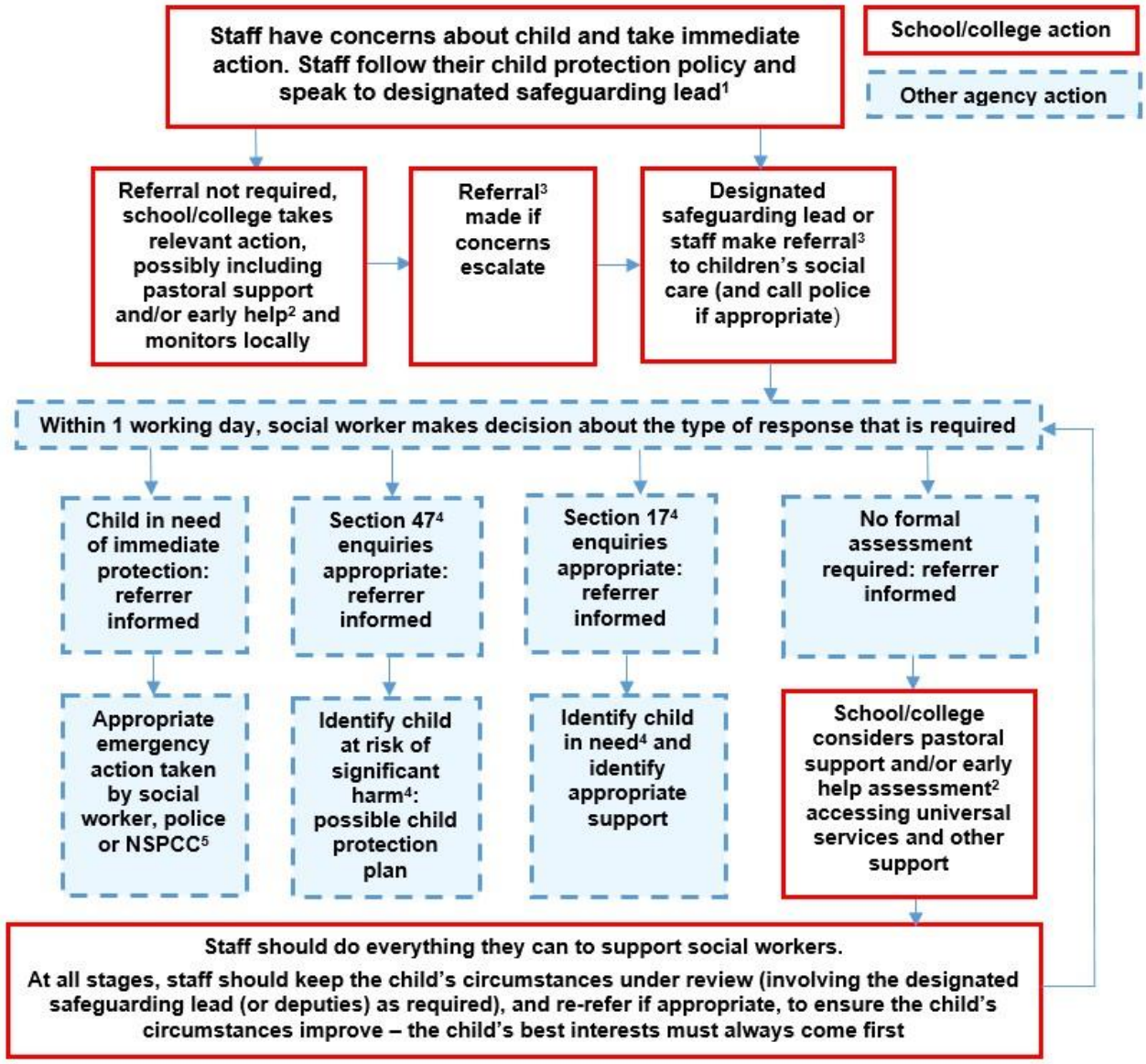
The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc. and make alternative provisions in advance where these might be needed.

At Windlesham School, we are aware of the potential risks resulting from the use of mobile and smart technology, particularly considering that many children have unlimited and unrestricted access to the

internet via mobile phone networks at home (i.e. 4G and 5G). This access means some children can potentially sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content including Deep Fakes. As the primary preventative measure to avoid such risks, Windlesham School does not permit pupils to have mobile or smart devices that contain a camera or live data feed at school. School staff will not use personal devices in the presence of children on the school premises.

6. Actions where there are concerns about a child's safety

The following flow chart is taken from page 24 of Keeping Children Safe in Education 2025 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



1 In cases which also involve a concern or an allegation of abuse against a staff member, see Part four of the guidance.

2 Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Working Together to Safeguard Children provides detailed guidance on the early help process.

3 Referrals should follow the process set out in the local threshold document and local protocol for assessment. See Working Together to Safeguard Children.

4 Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that

a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Working Together to Safeguard Children.

5 This could include applying for an Emergency Protection Order (EPO)

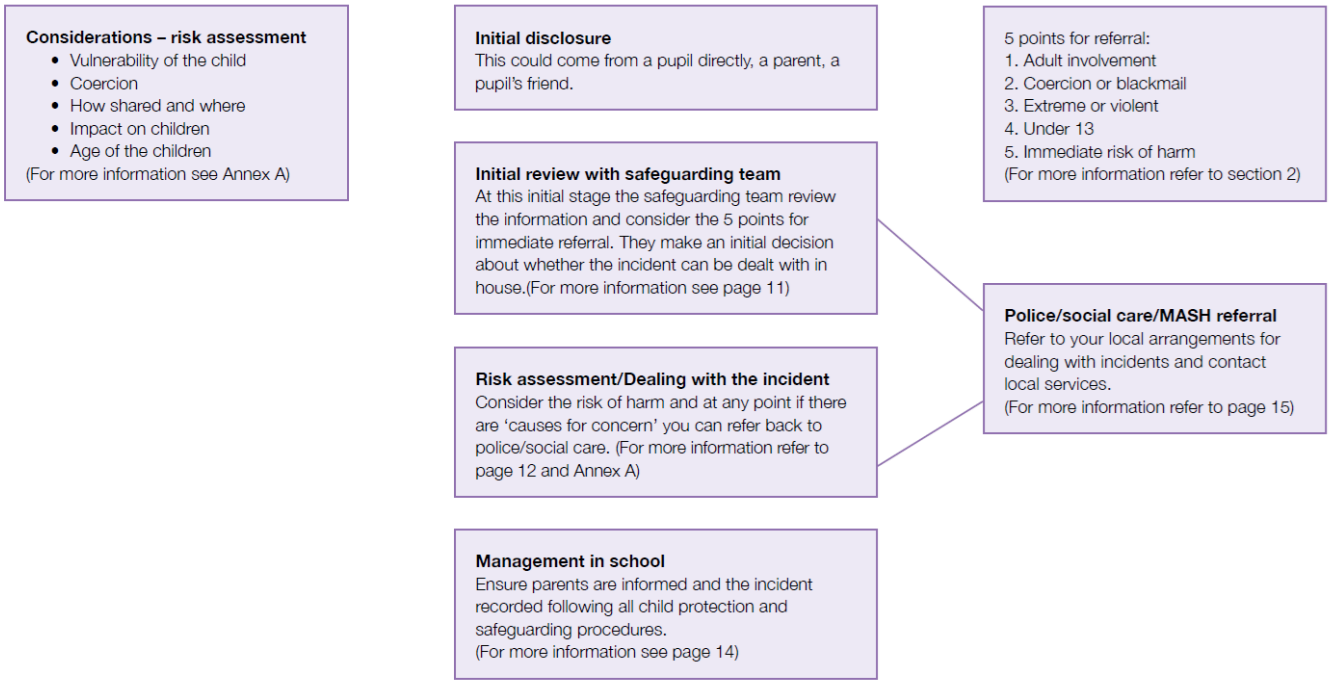
7. Sexting

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as 'youth produced sexual imagery') in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called Sexting; how to respond to an incident for all staff to read, in recognition of the fact that it is mostly someone other than the DSL or online safety lead to first become

Annex G

Flowchart for responding to incidents



aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL and/or the Headteacher must not attempt to share or delete the image or ask anyone else to do so, but to go straight to the DSL/Head.

The school DSL will in turn use the full guidance document, Sexting in Schools and Colleges to decide next steps and whether other agencies need to be involved. It is important that everyone understands that whilst

sexting is illegal, pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

The documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

8. Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education and that pupils can come and talk to members of staff if they have made a mistake or had a problem in this area.

9. Bullying

Online bullying 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.

10. Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

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. 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.

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

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These rules are clearly on display in the Computer Suite.

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platform and other technology.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff handbook.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any home learning that may take place in future periods of closure or quarantine etc.

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.

12. Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Windlesham community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school's behaviour policy (for pupils) or handbook (for staff).

Breaches by parents will be addressed on an individual basis, potentially with the involvement of the authorities.

Further to this, where an incident relates to an inappropriate, upsetting, violent or abusive social media post by a member of the school community, Windlesham 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 (run by the UK Safer Internet Centre) for support or help to accelerate this process.

13. Data protection and data security

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DSL will seek to apply. This quote from the latter document is useful for all staff:

"GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent (DPA, Part 2,18; Schedule 8, 4)

When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be

shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

The following data security products are used to protect the integrity of data, which in turn supports data protection Opentext Core Endpoint Antivirus, Opentext Threat Intelligence and Egress.

The Headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first, and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared with colleagues via approved channels (ie confidential entries on Engage). The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data with colleagues outside the School domain. If this is not possible, the DSL should be informed in advance.c

14. Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place and so that children are not able to access harmful or inappropriate material but at the same time should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." The appropriateness of any filtering and monitoring systems will be informed in part, by the Prevent Duty Risk Assessment.

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)
2. Internet and web access
3. Active technology monitoring services

At Windlesham, we have decided that all three options are appropriate for use throughout the school.

For a detailed list of the measures undertaken to comply with this requirement, please refer to Appendix 8, which lists the Cyber Security Standards and measures undertaken to comply with these.

15. Electronic communications

Please read this section alongside references to pupil-staff communications in the overall school Safeguarding Policy, and in conjunction with the Data Protection Policy. This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Staff and pupils (where appropriate) have school emails set up via Microsoft Office365. Pupil emails are inactive unless required for remote purposes. Year 6 may also have these as part of their computing curriculum.

The system is user name and password authenticated and therefore is fully auditable, trackable and managed by Virtual IT Education on behalf of the school. The use of MyLogin/Clever is planned for later this year, which incorporates unique user login via QR codes and SSO for all children, but NOT for staff. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email is (Microsoft Teams and the Parental portal via Engage) the only means of electronic communication to be used between staff and pupils and staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer and Headteacher in advance. 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).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.
    - If data needs to be shared with external agencies, Outlook encrypted and Egress systems.
    - Internally, staff should use the school network, including when working from home when remote access is available via Engage and the school-run Office365 system.
- All pupils are restricted to emailing within the school and cannot email external accounts.
- Appropriate behaviour is expected at all times, and the system should not be used to send inappropriate materials or language w`hich 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
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- Where a member of staff needs to email an individual pupil a member of SLT must be copied.

See also the social media section of this policy.

16. School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to the office admin staff and the PA to the headteacher. The site is managed and hosted by Inner Media.

The DfE has determined information which must be available on a school website. LGfL has compiled RAG (red-amber-green) audits at safepolicies.lgfl.net to help schools to ensure that are requirements are met (last carried out March 21).

Where other staff submit information for the website, they are asked to remember:

- School has 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 high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- Where pupil work, images or videos are published on the website, their identities are protected, and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

17. Cloud platforms

Windlesham uses the Microsoft's Office 365 system and our DPO (Mrs Roberts) can provide a copy of the school's most recent DP policy.

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager analyse and document systems and procedures before they are implemented and regularly review them.

The following principles apply:

- The DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact Assessment)
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Confidential Pupil data is only accessible to staff via the Engage Client platform. There is restricted access to Staff data, which is restricted to the Senior Leadership Team and certain administrative staff, this level of access is determined by the Headteacher and the DPO.
- Pupil images and videos are only made public with parental permission
- Only school-approved platforms are used by students 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)

18. Digital images and video

When a pupil joins the school, parents and carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long. Parents answer as follows:

- For the newsletter (which is uploaded onto the school website)
- For use in paper-based school marketing, such as fliers.
- For general marketing and publicity such as; online prospectus or websites
- For Schools social media (Facebook, Instagram)

Whenever a photo or video is taken or made, the member of staff taking it will check the latest database 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 their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones and personal equipment for taking pictures of pupils, and where these are stored.

At Windlesham, Photos are stored on the school network in line with the retention schedule of the school Data Protection Policy.

No images, videos or audio of children will be recorded on personal devices. Only school devices, subject to the school's filtering and monitoring systems will be used. In rare cases, with specific authorisation from the hear, photos can be taken in a personal phone, but images must be transferred and then removed from the personal device within 2 school days.

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at Parent Filming lgfl

We encourage young people to think about their online reputation and digital footprint, so we should be good adult role models by not oversharing (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 online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

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.

19. Social media - Windlesham's SM presence

Windlesham 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 the ISI pre-inspection check includes monitoring what is being said online.

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 to respond to criticism and praise in a fair, responsible manner.

Miss Ella Dean, Admissions Officer, is responsible for overseeing our Facebook and Instagram accounts and checking our Wikipedia and Google reviews. She follows the guidance in the Safer Internet Centre online-reputation management document here. The headteacher will assist with the content creation of the Instagram account.

20. 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 and as a school we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, 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, being mindful not just of content but also of tone. 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 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 ultimately detrimental to the pupils we serve).

Many social media platforms have a minimum age of 13 but on occasion the school deals with issues arising on social media with pupils under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that online harms regulation is likely to require more stringent age verification measures over the coming years.

However, the school has to strike a difficult balance between discouraging underage use of social media our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day). You may wish to refer to the Top Tips for Parents poster along with relevant items from parentsafe.lgfl.net and introduce the Children's Commission Digital 5 A Day.

The school has official Windlesham Facebook and Instagram accounts (managed by Miss Dean) and will respond to general enquiries about the school, but asks parents and 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.

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. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow public student 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.

Staff with personal social media accounts should regularly check their settings are set at an appropriate level to ensure that their personal content is secure.

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 of the 131 Prohibition Orders issued to staff in 2017, 73 involved social media/technology (and 27 of the 66 orders by August 2018).

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 page 25) and permission is sought before uploading photographs, videos or any other information about other people.

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the school's Data Protection Policy.

21. Device usage

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 acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

22. Personal devices including wearable technology and bring your own device (BYOD)

- **Pupils** in Year 6 are allowed to bring mobile phones in for emergency use only which are handed in to the main school office on arrival into school and picked up at the end of the school day. Wearable technology is also prohibited, eg fitbits
  Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section and Data protection and data security section. Staff data should never be downloaded onto a private phone.
- **Visitors, Volunteers, contractors, governors** should leave their phones in their pockets and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos. If this is required (e.g. for contractors to take photos of equipment or buildings), permission of the Headteacher should be sought (the Headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. Parent Filming lgfl may provide further useful guidance]. Parents are asked

not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

23. Network and internet access on school devices

- **Pupils** are not allowed networked file access via personal devices.
- **Staff** are now allowed access to the school Wi-Fi on one mobile devices to enable people to get hold of them during the school day. The password is not shared but instead directly inputted by the headteacher of other SLT.
- **Staff home devices** are allowed with specific consent from the headteacher or DPO where these are used Soley for work purposes. This may be connected to main wifi.
- **Guest Home devices** are generally not allowed in school. On the rare occasion this has been sanctioned by the Headteacher or the DPO access to a guest wifi network only.
- **Volunteers, contractors, governors** can access the guest wireless network but have no access to networked files or drives, subject to the acceptable use policy. All internet traffic is monitored through the school's Smoothwall monitoring systems
- **Parents have** no access to the school network or wireless internet on personal devices. Occasionally, when requested this can be facilitated and the guest wireless network only without access to networked files or drives, subject to the acceptable use policy. All internet traffic is monitored.

24. Trips and events away from school

Staff should never use their personal devices to record images or videos of children at school.
Whenever staff attend an out of school event, they should endeavour to take the School mobile phone. This may be used to record video, take images and to contact parents or the school as necessary.
If the School mobile is not available, staff should seek authorisation in writing from the Headteacher to use their personal devices specifically for the event requested. The extent of usage will be decided by the Headteacher based on the circumstances of the trip.
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 student accessing a teacher's private phone number.

25. Searching and confiscation

In line with the DfE guidance (Jan 2018) 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils and their property on school premises. 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.

Please refer to Section 14 of the School's Behaviour Policy.

Appendices

- EYFS Policy for the use of cameras and mobile phones and devices
- Staff, Governors and Visitors AUP Form
- Pupil AUP Form
- Parental AUP Letter
- Flow chart outlines actions for unsuitable or illegal materials
- User Actions acceptability continuum
- Safeguarding (including online safety) Incident log via Engage
- Cyber Security Standards
- DRAFT Safeguarding Policy 2025-2026
- Behaviour Policy Jan 2025
- Anti-Bullying Policy
- Staff Handbook (internal Engage system)
- Online-Safety Questions from the Governing Board (UKCIS)
- Education for a Connected World cross-curricular digital resilience framework (UKCIS)
- Safer working practice for those working with children & young people in education (Safer Recruitment Consortium)
- Working together to safeguard children (DfE)
- Searching, screening and confiscation advice (DfE)
- Sexual violence and sexual harassment between children in schools and colleges (DfE advice)
- Sexting guidance from UKCIS
- Prevent Duty Guidance for Schools (DfE and Home Office documents)
- Preventing and tackling bullying (DfE)
- Cyber bullying: advice for headteachers and school staff (DfE)

APPENDIX 1 – EYFS Policy for the use of cameras and mobile phones and devices

To ensure the safety and welfare of the children in our care, this policy outlines the protocols for the use of personal mobile phones/devices and cameras in the EYFS setting at Windlesham School.

Personal mobile phones, cameras and video recording equipment cannot be used when in the presence of children on school premises including the swimming pool.

· All mobile phones must be stored securely out of reach within the setting during contact time with children. This applies to staff, visitors, parents, volunteers and students.

· No parent is permitted to use their mobile phone or use its camera facility whilst inside school buildings, in the swimming pool or around the grounds when children are present.

· Mobile phones must not be used in any teaching area within the setting or within the bathroom area.

· In the case of a personal emergency, staff should use the school telephone. It is the responsibility of all staff to make families aware of the school telephone numbers.

· Personal calls may be made in non-contact time but not within the teaching areas.

· Personal mobiles, cameras or video recorders should not be used to record classroom activities. School equipment only should be used.

· Photographs and recordings can only be transferred to and stored on a school computer/IPad or laptop before printing.

· All telephone contact with parents and carers should be made on the school telephone.

· During group outings, nominated staff will have access to the school mobile which can be used in an emergency or for contact purposes. Staff may carry their own phones in bags but they should only be used in emergencies.

· In the case of school productions and sports day, parents and carers are permitted to take photographs/video footage of their own child in accordance with school protocols but we strongly advise against the publication of any such photographs on social networking sites. Most EYFS events will be videoed / photographed by school staff and then made available to paren

APPENDIX 2 – Staff, Governors and Visitors AUP Form

Acceptable use of the school's ICT facilities and the internet: agreement for staff and governors
Name of staff member/governor:
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote any private business, unless that business is directly related to the school
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will ensure that when I leave my workstation that the computer is locked to prevent any unauthorised access. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date:

26.
APPENDIX 3 - Pupil AUP Form

This is now completed on the school website and the latest link for this can be seen below.

https://www.windleshamschool.co.uk/aup/

APPENDIX 4 – Parental AUP Letter

Dear Parent/ Carer

ICT including the Internet, email and mobile technologies has become an important part of learning. We expect all children to be safe and responsible when using any ICT at Windlesham School.

Please read and discuss the enclosed online safety rules with your child and sign and return the slip. If you have any concerns or would like further information please contact me on 01273 553645

Thank you for your help on this important matter.

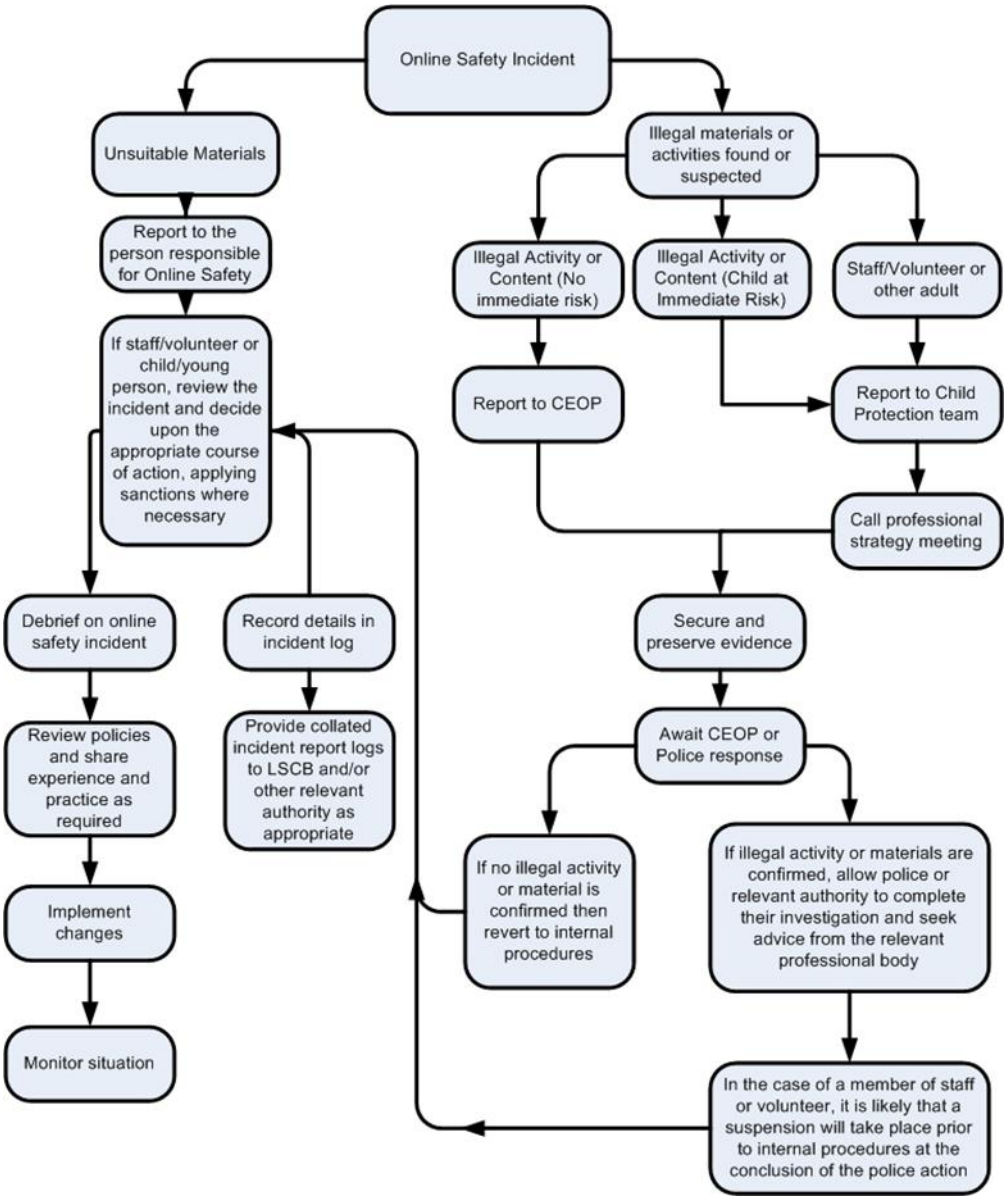
Yours sincerely

Windlesham School & Nursery

Mr Nick Matthews

Online Safety Co-ordinator

APPENDIX 5 – Flow chart outlines actions for unsuitable or illegal materials



APPENDIX 6 – User Actions acceptability continuum

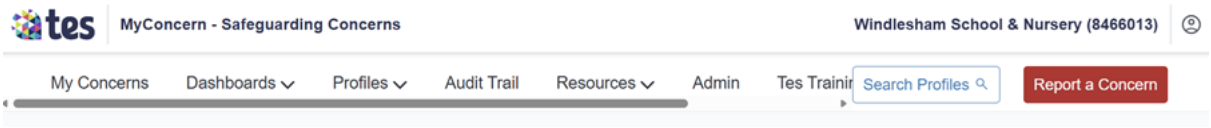
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce			X			
File sharing			X			
Use of social media			X			

Use of messaging apps		X			
Use of video broadcasting eg Youtube		X			

APPENDIX 7 – How to log a safeguarding concern on MyConcern

Logon to My Concern: https://myconcern.thesafeguardingcompany.com

Click on the red 'Report a Concern' button



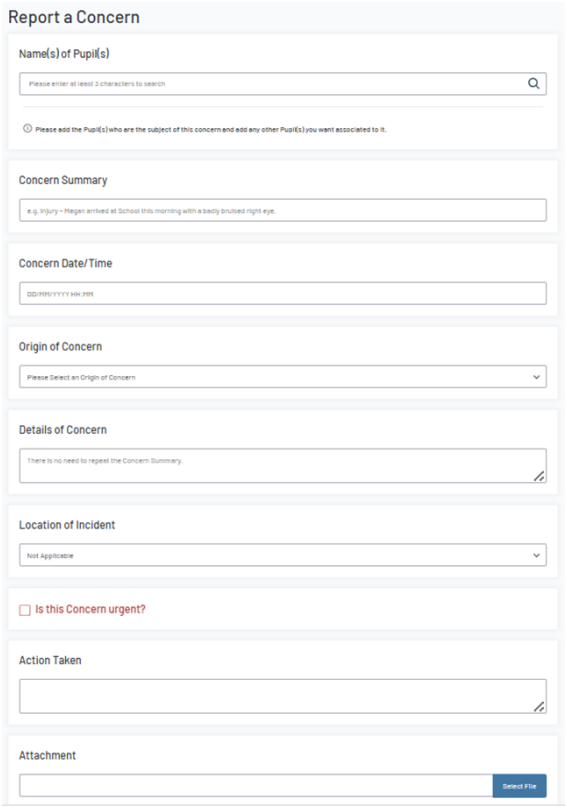
This will take you to 'Report A Concern'. Here you will need to go through each section and answer the question. Please ensure that you complete each question using facts and if you are stating an opinion, then please ensure that you refer to this as an opinion.

The summary is very important. Make this brief but clear about what the concern is.

Action taken refers to what you have already done because of this. Please include anything you have done here.

Please ensure that the incident date reflects when the incident happened, not when you completed the form.

Click **submit** once completed and this will send this to the DSL team.

- 

APPENDIX 8

Cyber Security Standards and measures to meet them:

1 Protect all devices on every network with a properly configured boundary or software firewall

Lightspeed filtering in place which covers all School devices.

2 Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date

Updates pushed on a schedule via Microsoft Intune policies

3 Accounts should only have the access they require to perform their role and should be authenticated to access data and services

365 groups define roles and data access.

4 You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication

MFA is setup for all staff email accounts

5 You should use anti-malware software to protect all devices in the network, including cloud-based networks

Sophos antivirus used by the School

6 An administrator should check the security of all applications downloaded onto a network

Software cannot be installed by users, all software is pushed out by Virtual IT Education

7 All online devices and software must be licensed for use and should be patched with the latest security updates

School has Microsoft A3 agreement for licensing and updates are pushed out on a schedule.

8 You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site

School has Opentext cloud to cloud backup for offsite and onsite, encrypted onsite and has a 90 day retention policy both onsite and offsite.

9 Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack

Backups are checked and tested weekly

10 Serious cyber attacks should be reported

These should be reported to Virtual IT Education and also the Police cyber security team.

Virtual IT Education emergency contact: escalations@virtualit.education

Main office number during working hours Monday-Friday 8-5 01903 767122
Out of hours – Simon Williams (07920045731)

Police Cyber Security Team – Dial 999 or
https://www.met.police.uk/advice/advice-and-information/fa/fraud/business-fraud/

11 You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation

The DPIA is currently being investigated SR

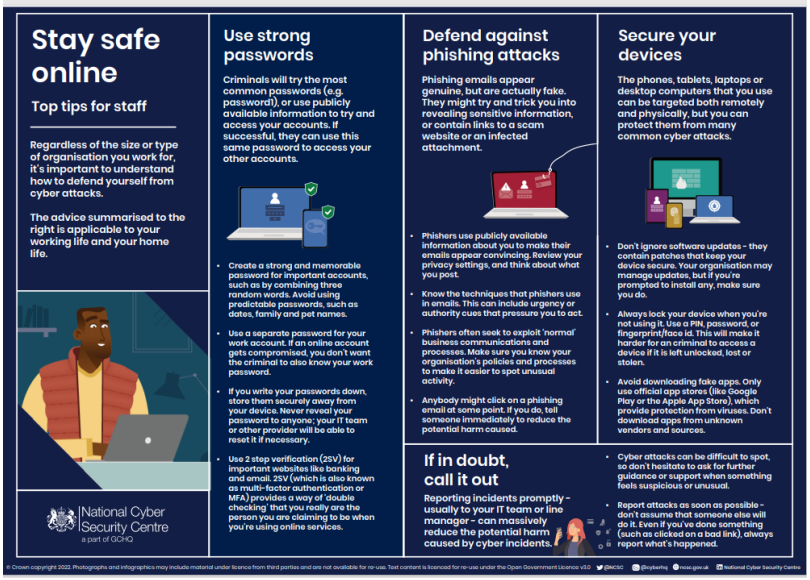
12 Train all staff with access to school IT networks in the basics of cyber security

https://www.ncsc.gov.uk/information/cyber-security-training-schools
(this is a 35 minute video with certificate issued at the end)

13 Protect all devices on every network with a properly configured boundary or software firewall

EXA Quantum in place

APPENDIX 9 Cyber Security



National Cyber Security Centre

Phishing attacks

Dealing with suspicious emails

Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). This advice includes tips about how to spot the most obvious signs of phishing, and what to do if you think you've clicked a bad link. For more information, please visit **www.ncsc.gov.uk/phishing** .

What is phishing?

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to **millions of people**, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

Make yourself a harder target

Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:

- Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.
- Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.
- If you have received an email which you're not quite sure about, forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk

What to do if you've already clicked ?

The most important thing to do is not to panic. There are number of practical steps you can take:

- Open your antivirus (AV) software, and run a full scan. Follow any instructions given.
- If you've been tricked into providing your password, you should change your passwords on all your other accounts.
- If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt.

- Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?
- Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly.
- If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq