



## Online Safety Policy

Last Reviewed: March 2023

Next Review Due: December 2023

Reviewed by:

John Ingrassia, Headteacher

Jack Cornish, Governor

Graham Rowlands-Hempel, Chair of Governors (Safeguarding)

Christine Mannion-Watson, Governor


## Contents

Contents .....	2
Introduction .....	1
Key people & dates .....	1
What is the policy? .....	1
Who is it for; when is it reviewed? .....	2
Who is in charge of online safety? .....	2
What are the main online safety risks today? .....	2
How will this policy be communicated? .....	2
Overview .....	4
Aims .....	4
Further Help and Support .....	4
Scope .....	4
Roles and responsibilities .....	4
Headteacher – Mr Ingrassia .....	5
Designated Safeguarding Lead & Online Safety Lead – Mrs S Kiernan.....	6
Governing Body, led by Online Safety & Safeguarding Link Governor – Mr Rowlands-Hempel.....	8
All staff .....	9
PSHE & RHSE Lead – Mrs Mills .....	10
Computing Lead – Mme Flynn .....	10
Subject leaders .....	11
Network Manager – JSPC .....	11
Data Protection Officer (DPO) – Mrs Roberts .....	12
Volunteers and contractors (including tutors).....	12
Pupils .....	13
Parents and carers.....	13
External groups including parent associations – Friends of Windlesham .....	13
Education and curriculum .....	14
Handling online-safety concerns and incidents.....	15
Actions where there are concerns about a child’s safety .....	16
Sexting .....	17

Upskirting .....	18
Bullying .....	18
Sexual violence and harassment .....	18
Misuse of school technology (devices, systems, networks or platforms) .....	18
Social media incidents .....	19
Data protection and data security .....	20
Appropriate filtering and monitoring .....	21
Electronic communications .....	21
Email .....	21
School website .....	22
Cloud platforms .....	22
Digital images and video .....	23
Social media - Windlesham's SM presence .....	24
Staff, pupils' and parents' SM presence .....	24
Device usage .....	26
Personal devices including wearable technology and bring your own device (BYOD) .....	26
Network and internet access on school devices .....	26
Trips and events away from school .....	27
Searching and confiscation .....	27
Appendices .....	28
APPENDIX 1 – EYFS Policy for the use of cameras and mobile phones and devices .....	29
Windlesham School Pupil Home/School ICT/AUP Agreement .....	33
----- .....	33
Windlesham School Pupil Home/School ICT Agreement .....	33

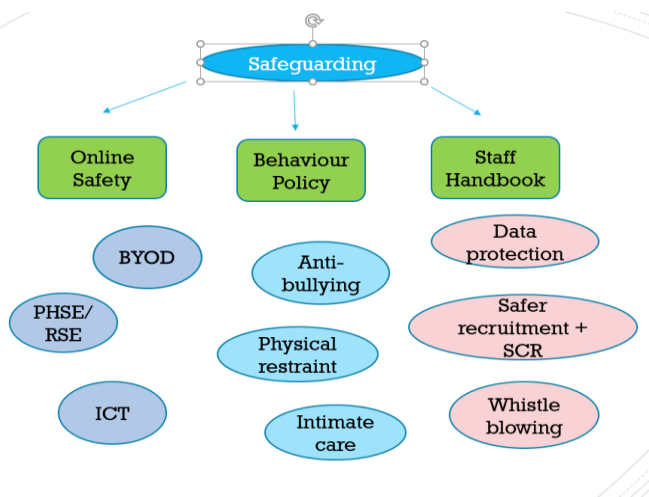
## Introduction

### Key people & dates

 Windlesham School	Designated Safeguarding Lead (DSL)	Mrs Sinead Kiernan
	Online-safety & safeguarding link governor	Mr Graham Rowlands-Hempel
	PSHE/RHSE lead	Mrs Mills
	Network manager	External agency – <a href="#">JSPC</a>
	Date this policy was reviewed and by whom	November 22 by, Mr John Ingrassia, Mr Jack Cornish & Mr Graham Rowlands-Hempel
	Date of next review and by whom	November 23 – Headteacher

### 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' 2020 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 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, regulations and Windlesham School aims to involve staff, governors, pupils and parents 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 will collaborate with the Head, the ICT co-ordinator, 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 2021, 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 of your pupils may have missed opportunities to disclose such abuse during the first lockdown.

## 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 network
- Available in paper format in the staffroom
- 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, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms and corridors
- Reviews of this online-safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement

## Overview

### 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, and 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 today's 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 your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs, 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). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

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.

### 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.

### 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 Ingrassia

### Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see [coronavirus.lgfl.net/safeguarding](https://coronavirus.lgfl.net/safeguarding) for an addendum to policies and an infographic overview of safeguarding considerations for remote teaching technology).
- 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
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information.
- 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), DSL 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 ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles (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



## Designated Safeguarding Lead & Online Safety Lead – Mrs S Kiernan

**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 2020):

- “The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] ... this **lead** responsibility should not be delegated”
- 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.” – see [safetraining.lgfl.net](https://safetraining.lgfl.net) and [prevent.lgfl.net](https://prevent.lgfl.net)
- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and the strategy on which they are based (in harmony with policies for behaviour, safeguarding, Prevent and others) and submit for review to the governors/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends – see [safeblog.lgfl.net](https://safeblog.lgfl.net) for examples or sign up to the [LGfL safeguarding newsletter](https://lgflsafeguarding.com)
- 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 Graham Rowlands-Hempel) 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.

- 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 provided by [Censornet](#). Details of which can be accessed [here](#).
- Ensure the [2021 Department of Education \(DfE\) guidance on sexual violence and harassment](#) is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
  - all staff must read KCSIE Part 1 and all those working with children Annex A
  - it would also be advisable for all staff to be aware of Annex D (online safety)
  - cascade knowledge of risks and opportunities throughout the organisation

## Governing Body, led by Online Safety & Safeguarding Link Governor – Mr Rowlands-Hempel

### 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 staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex A; check that Annex C on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- 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.

## All staff

### Key responsibilities:

- Pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies** (see [coronavirus.lgfl.net/safeguarding](https://coronavirus.lgfl.net/safeguarding) for an infographic overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP.
- Recognise that RSHE is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- 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 – Mrs S. Kiernan
- Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for 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
- Notify the DSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities 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)
- When 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
- 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.

## **PSHE & RHSE Lead – Mrs Mills**

### **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 ICT curriculum is available to all year groups
- Work closely with the Humanities lead to avoid overlap but ensure a complementary whole-school approach
- 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 – JSPC

### Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and 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 new 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

## Data Protection Officer (DPO) – Mrs Roberts

### Key responsibilities:

- NB – this document is not for general data-protection guidance;
- Liaise with JSPC 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.

## 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)
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- 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) and read the pupil AUP and encourage their children to follow 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.
- Encourage children to engage fully in home-learning during any period of remote learning or bubble or school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.
- 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

## 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](https://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.

## 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 Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policies (including Staff BYOD)
- 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.

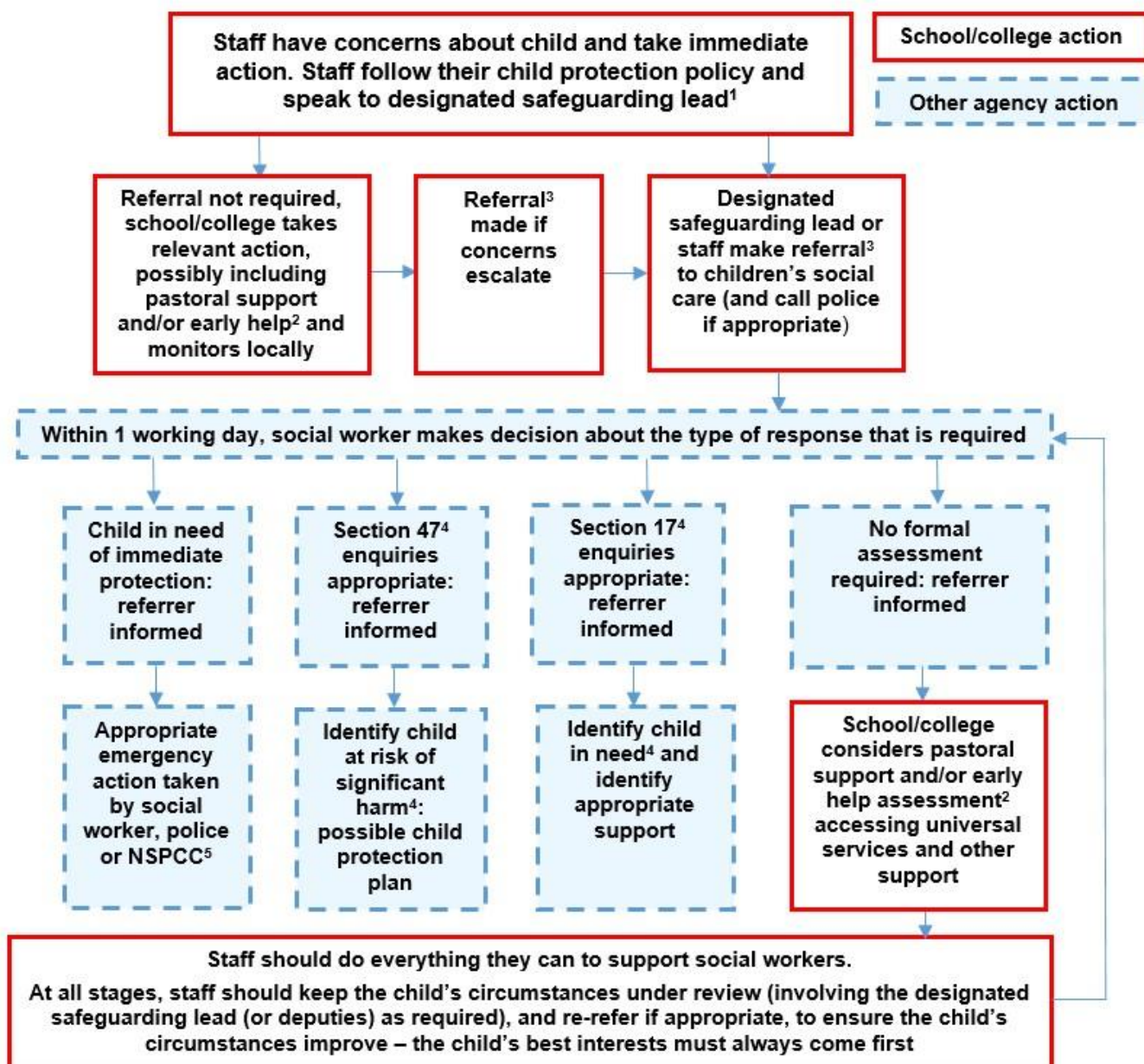
Any concern or allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors [governors@windleshamschool.co.uk](mailto:governors@windleshamschool.co.uk) and the LADO (Local Authority's 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.

## Actions where there are concerns about a child's safety

The following flow chart is taken from page 13 of Keeping Children Safe in Education 2020 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.



## 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.

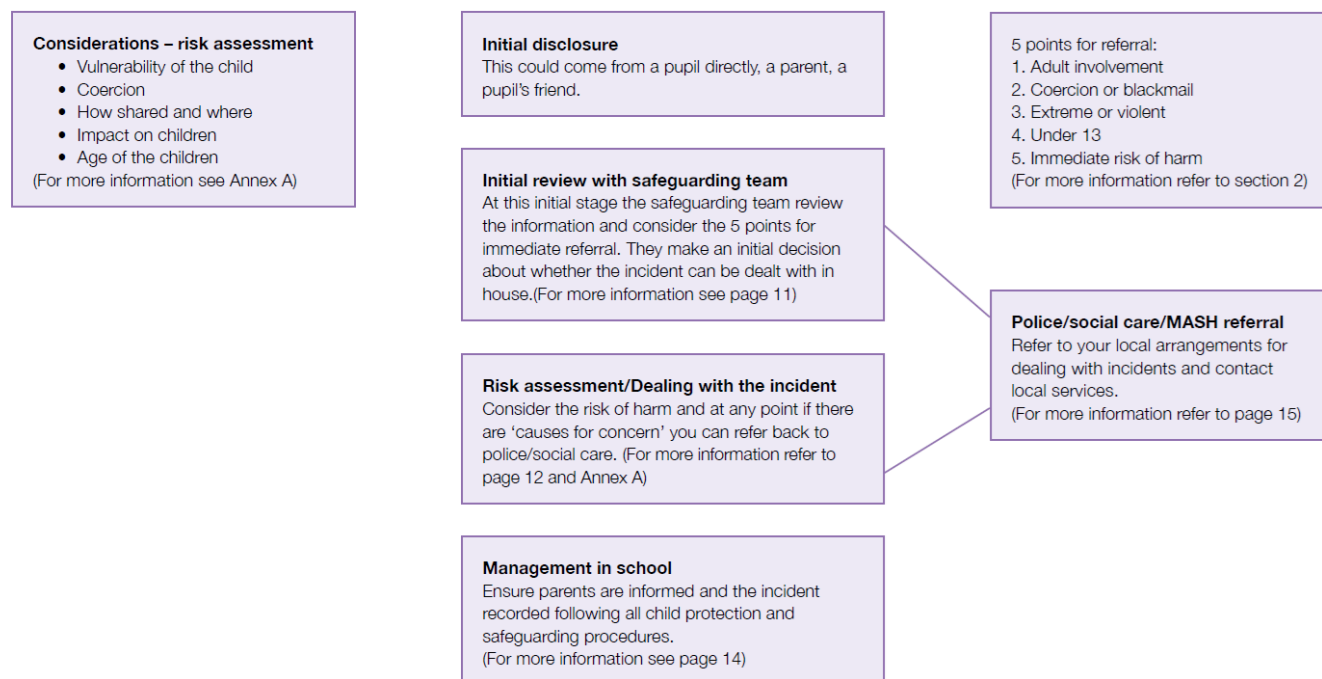
There is a one-page overview called [Sexting; how to respond to an incident](#) for all staff to read, in recognition of the fact that it is mostly someone other than the DSL or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than 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](http://sexting.lgfl.net)

## Annex G

### Flowchart for responding to incidents



## **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.

## **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.

## **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.

## **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 ICT room.

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, as well as to Staff BYOD (bring your own device) policy.

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.

## **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.

## Data protection and data security

Data Protection information on the relationship between the school and Learning Grid for Learning (LGfL) can be found at [gdpr.lgfl.net](https://gdpr.lgfl.net); there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

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 Sophos Anti-Virus, Sophos Anti-Phish, Sophos InterceptX, Sophos Server Advance, Malware Bytes 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 via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data. If this is not possible, the DSL should be informed in advance.

## 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 be 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.”

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.

On the rare occasion when a pupil is allowed to bring a personal device into school and log onto a school system this can be monitored via the above systems.

## 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 use these as part of their ICT curriculum.

The system is user name and password authenticated and therefore is fully auditable, trackable and managed by Mr Ferries on behalf of the school. 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 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
- 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.

## 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. The site is managed and hosted by [Rowena](#).

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 requirements are met (last carried out March 21). Note that an RSHE policy is now included.

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

- School 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 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).

## 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 statement) and parental permission is sought

- 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
- Pupil data is only accessible to staff via the Engage Client platform. There is restricted access to Staff data 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)

## 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, members of staff authorised by the Headteacher, may occasionally 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, as per the School's Staff BYOD policy

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

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 [parentfilming.lgfl.net](http://parentfilming.lgfl.net)

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.

## **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](mailto: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.

Mrs Croucher, Deputy Head, 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](#).

## **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 (note that WhatsApp is 16+), 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](http://parentsafe.lgfl.net) and introduce the [Children's Commission Digital 5 A Day](#).

The school has official Windlesham Facebook and Instagram accounts (managed by Mrs Croucher/Mrs ) 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/Principal, 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 23) 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.

## 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.

## 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 on page 23 and Data protection and data security section on page 20. Staff data should never be downloaded onto a private phone.
- **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 on page 23. [[parentfilming.lgfl.net](http://parentfilming.lgfl.net) 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.

## Network and internet access on school devices

- **Pupils** are not allowed networked file access via personal devices.
- **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.
- **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 on page 23 and Data protection and data security section on page 20. Child/staff data should never be downloaded onto a private phone.

- Windlesham does operate a BYOD policy for Staff. (see appendix)
- **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.
- **Parents** generally 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.

## **Trips and events away from school**

For school trips and events away from school, teachers will 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 student accessing a teacher's private phone number.

## **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

1. EYFS Policy for the use of cameras and mobile phones and devices
2. Staff Agreement on the use of BYOD at School
3. Staff, Governors and Visitors AUP Form
4. Pupil AUP Form
5. Parental AUP Letter
6. Flow chart outlines actions for unsuitable or illegal materials
7. User Actions acceptability continuum
8. Safeguarding (including online safety) Incident log via Engage
9. [Safeguarding and Child Protection Policy](#)
10. Behaviour Policy
11. [Anti-Bullying Policy](#)
12. Staff Handbook (internal Engage system)
13. [Online-Safety Questions from the Governing Board \(UKCIS\)](#)
14. [Education for a Connected World cross-curricular digital resilience framework \(UKCIS\)](#)
15. [Safer working practice for those working with children & young people in education \(Safer Recruitment Consortium\)](#)
16. [Working together to safeguard children \(DfE\)](#)
17. [Searching, screening and confiscation advice \(DfE\)](#)
18. [Sexual violence and sexual harassment between children in schools and colleges \(DfE advice\)](#)
19. [Sexting guidance from UKCIS](#)
20. [Prevent Duty Guidance for Schools \(DfE and Home Office documents\)](#)
21. [Preventing and tackling bullying \(DfE\)](#)
22. [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 parents.



## APPENDIX 2 – Staff Agreement on the use of BYOD at School

In a Smart School, one in which newer technologies are exploited to improve its provision, prohibiting all staff from using personal devices (BYOD - Bring Your Own Devices) may not always be in the best interest of children, parents, teachers, visitors or the School. There are many examples when the use of a personal device by a member of staff in the presence of children is justified, and with the right measures taken, does not pose any greater threat of exploitation than the use of any school device.

This agreement sets out measures which the School will take to minimise safeguarding risks in circumstances when a member of staff is authorised to use their phones in the presence of children.

It will also include reasons which justify the use of personal devices at School and the conditions which any member of staff must agree to in order to reduce any risks posed. This policy also sets out how the use of a personal device may be authorised for use.

Any member of staff or visitor not granted specific consent to use their BYOD's at school in line with this agreement, must continue to adhere with the terms set out in the **Online Safety Policy**. In brief, these require staff phones to not be visible in the presence of children and never to be used for capturing images, or for communicating with children or parents.

Personal use (calls, social media, emails and messages for example) should not be via a school Wifi network and should only take place in a private environment.

Phones should always be silenced or switched off in the presence of children, at staff meetings or other professional settings.

### Examples of authorised use of BYOD

Examples of authorised use of BYOD include but are not limited to:

1. When a member of staff is on a school trip or residential and an iPad is not practical to carry around. At such times, it may be more convenient to use one's own device to capture quality images and to make phone calls or send messages to colleagues which ensure the safe and smooth running of the trip.
2. To capture quality images of children in different contexts, it is often easier if one has access to one's own device and such images are often of a better quality to those available at school.
3. To create a marketing promotion requiring higher levels of image quality or the ease of editing associated with a BYOD.
4. To record images at sporting fixtures to share quickly with the social media liaison officer.
5. When a school device is not available and an opportunity to capture a special learning moment presents itself.

### Measures to minimise risk

1. During school hours, authorised personal devices may only be used to access files on internet sites which are relevant to the classroom curriculum.
2. BYOD are not to be used in the pool area, viewing gallery, toilets, bathrooms and changing rooms or in the vicinity of any intimate care provision.
3. The recording, taking and sharing of images, video and audio on a BYOD must conform with the **Use of digital and video images section** of the **Online Safety Policy**.
4. All Staff, including volunteers, should not use their own personal mobile phone for contacting children or parents and carers, unless it is an emergency or they are unable to use the school telecoms systems.

### Conditions of consent to use BYOD for school related activities

1. Only devices authorised by the Headteacher may be used to take photographs/videos, send/receive messages or take calls in the presence of children.

2. Any authorised device must be secured with access protection: pin, fingerprint recognition, eye scan or similar.
3. No staff device will be given access to the school local network or Wifi network (the School Guest wifi network can be accessed).
4. Images must only be taken for the purpose of use within the school including social media, not for personal use.
5. If it is necessary for a phone call or text to be taken or received, care should be taken to avoid disturbance or disorder to the running of the school.
6. **The school reserves the right to request random checks of the device.**
7. Any images captured on the device should be immediately uploaded to the school SharePoint account and deleted from the device as soon as the upload is complete.
8. BYOD's should never be used to capture images for safeguarding concerns e.g. bruising, scratches etc. Only school devices can be used for this.
9. Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the School Office.

Any member of staff who wishes to use their own device for professional purposes such as those outlined above must complete an 'Authorised use of BYOD at School' form, at Appendix A.

## **Appendix A**

### **Authorised use of BYOD at School**

#### **Staff:**

I accept and agree to comply with the terms set out in this agreement.

Specifically, I agree to:

- My phone being checked by the school if requested
- Uploading images and video footage taken of children to SharePoint
- Maintaining high levels of access security on my device
- Not passing my phone to other members of staff or other adults to take photos of children on my behalf
- Not using any other device, other than that which is authorised to take such images as comply with the guidance specified in the eSafety Policy and described below.

**The phone/device Registered for Use is (please provide details necessary to identify device):**

---

**Name and signature of staff member:**

---

**Date:**

---

**Agreed by Headteacher:**

---

**Date:**

---

## Windlesham School ICT Acceptable Use Agreement: Staff, Governors and Visitors

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Bursar.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the ICT Co-Ordinator
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

### User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ..... Date .....

Full Name .....(printed)

Job title .....

**Windlesham School Pupil Home/School ICT/AUP Agreement**

- I will only use ICT in School for School purposes
- I will not download games or other software at School
- Where email is used as part of the curriculum I will only use my class email address or my own School email address when emailing
- I will only open email attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will not visit chatrooms or discussion forums other than those which are academically based and approved by the School as beneficial to my work
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my screen and tell my teacher immediately
- I will not give out my own details such as my name, phone number or home address
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I know that my use of ICT can be checked and my parent/ carer contacted if a member of School staff is concerned about my eSafety

-----

**Windlesham School Pupil Home/School ICT Agreement**

We have discussed this and  
.....(child’s name - please print) agrees to follow the eSafety rules  
and to support the safe use of ICT at Windlesham School.  
Parent/ Carer Signature .....  
Date .....

## APPENDIX 5 – 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.

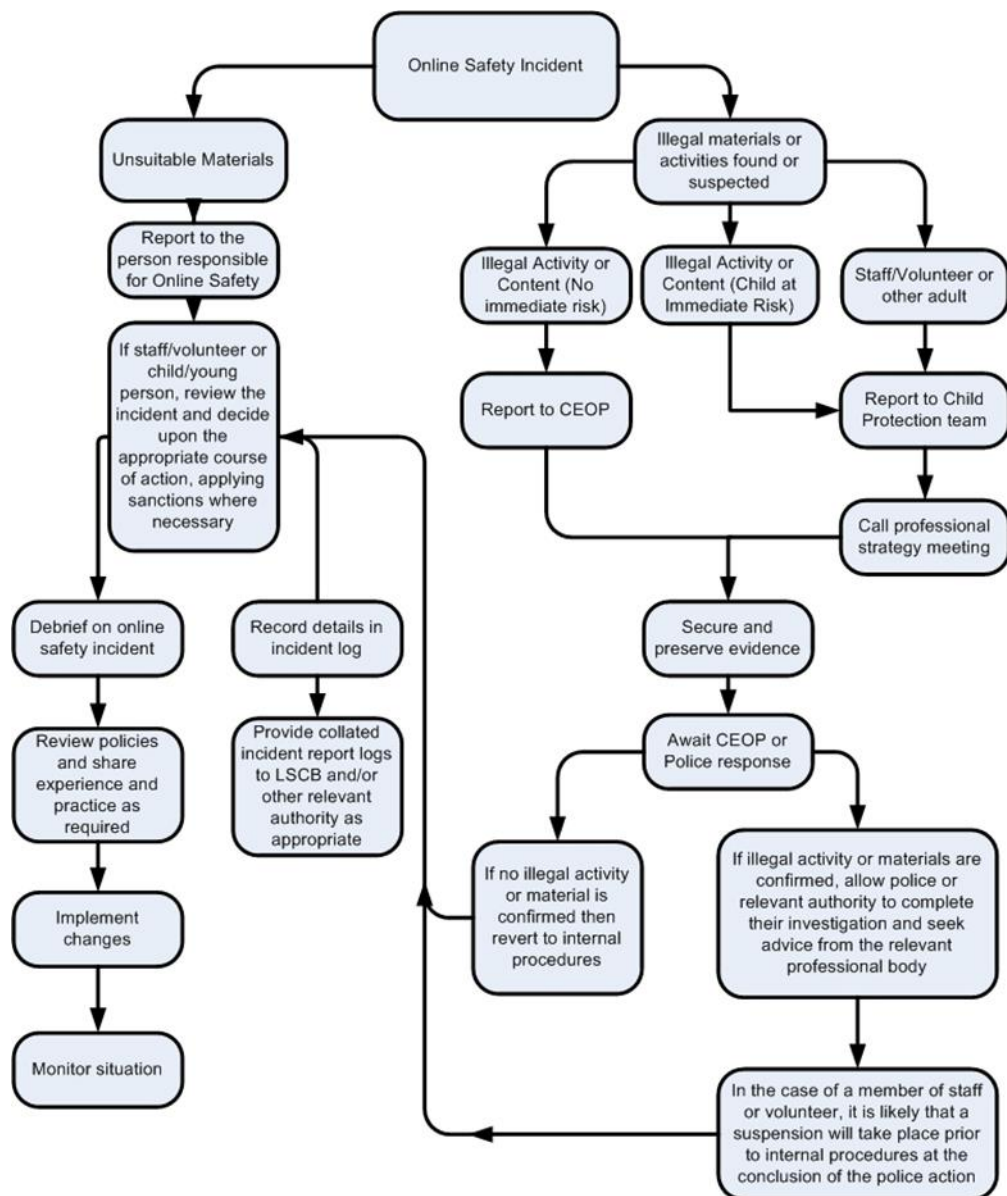
Please read and discuss the enclosed online safety rules with your child and sign and return the slip. If you have any concerns or would like some explanation please contact me on 01273 553645.

Thank you for your help on this important matter.

Yours sincerely

Mrs Samantha Roberts  
Online Safety Co-ordinator

## APPENDIX 6 – Flow chart outlines actions for unsuitable or illegal materials



## APPENDIX 7 – User Actions acceptability continuum

### User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
<b>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:</b>	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			

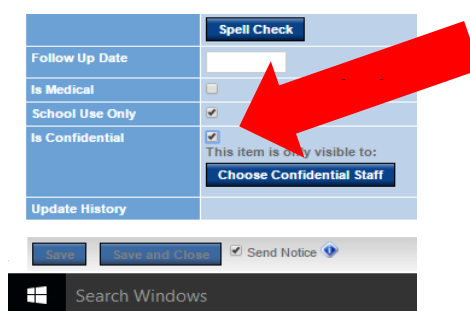
## APPENDIX 8 – How to log a safeguarding concern

### **How to Raise a Safeguarding Concern (including Online Safety Concern) – August 2021**

1. Open Engage, Daybook Entry
2. Click 'Add New Entry' and select 'Incident'
3. Select pupil and move across into 'selected Pupil Recipients' box.
4. In the drop down menu of Incident Type, select 'Safeguarding Concern'
5. Your name and date should already be in the boxes – just add the time
6. In the details box outline the main points of information:

**When did this occur? Where did this occur? Who is involved? What happened?**

7. Add any linked pupils
8. Then CLICK the CONFIDENTIAL BOX



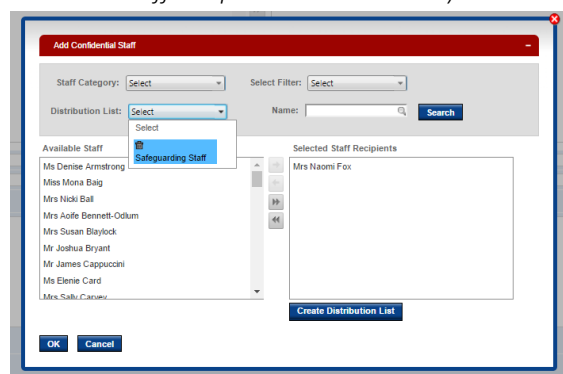
It will give you the option to select the staff that this is sent to

9. Select the staff (current list at the bottom on this sheet) and move across into the 'Selected Staff Recipients' and press 'OK'.

*(You can create a Distribution List which will save you time in the future.*

*Click 'Create Distribution List' move staff across, name it 'Safeguarding Staff' and then click 'OK' A current list of Safeguarding key staff will appear and transfer them into the 'Selected Staff Recipients' and Press 'Ok')*

10. Ensure that the 'Send Notice' box is ticked
11. Press Save
12. You are then able to attach any photographs or notes



Please note that this will no longer be visible to you but you will receive and acknowledgment from the member of staff that deals concern the **same day**.

Staff to include: **Pupil Safeguarding** – Mrs S. Kiernan (DSL), Mr J. Ingrassia (Deputy DSL) & Mrs R. Older (EYFS) & Deputy DSL

**Allegations about staff:** Mr J Ingrassia

**Allegations about the SLT :** Mr Graham Rowlands-Hempel [governors@windleshamschool.co.uk](mailto:governors@windleshamschool.co.uk)