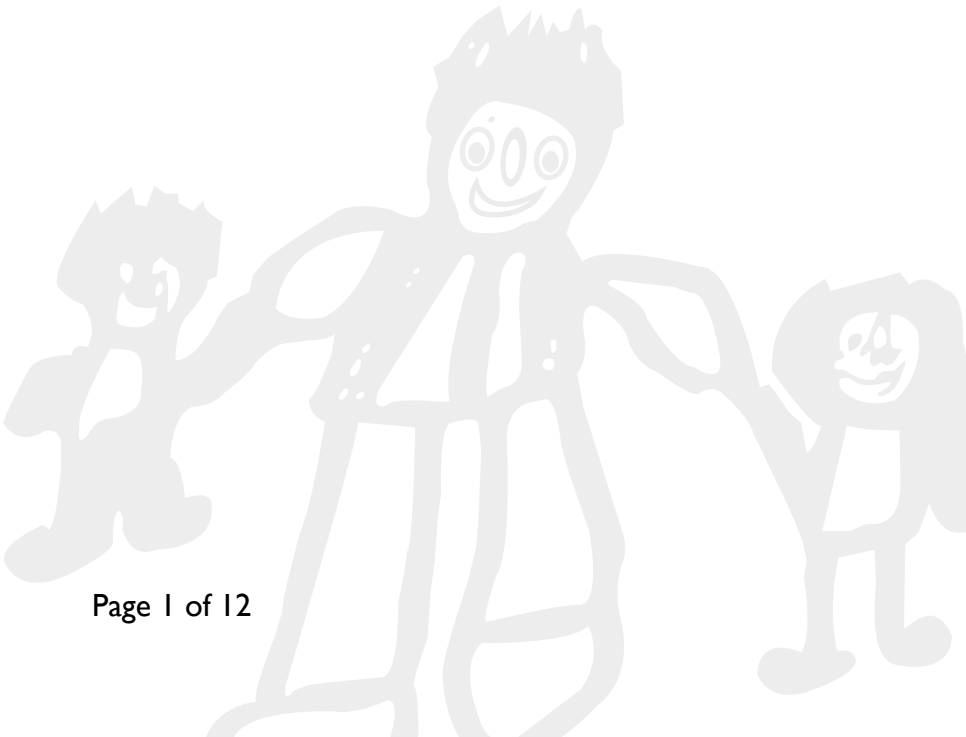
Online Safety (Draft)



Introduction

Frank Wise School recognises that technology and the use of ICT equipment is part of everyday life and that it is now an essential part of leisure, learning and employment. ICT systems are one of the fastest and most effective ways of finding information, sharing ideas and working with other people, but whilst effective there are also risks.

As part of our safeguarding responsibility, we aim to protect all staff and pupils against risks associated with the internet and other technology aids, such as mobile phones.
This will include:

- Having robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Delivering an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establishing clear mechanisms to identify, intervene and escalate an incident, where appropriate

Scope of the Policy

This policy applies to all members of the Frank Wise School community (including staff, students/ pupils, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology equipment and content, both in and out of the school.

Legislation and Guidance

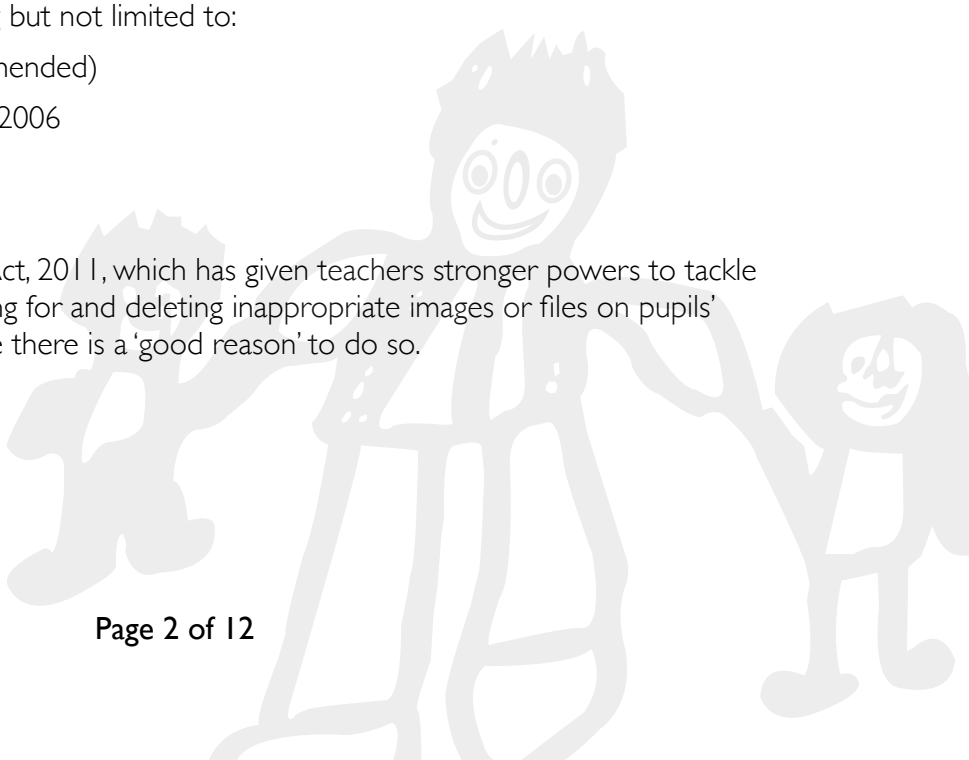
This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools, June 2019
- Preventing and tackling bullying, July 2017
- Cyberbullying: advice for headteacher and school staff
- Relationships education, relationships and sex education (RSE) and health education, July 2019
- Searching, screening and confiscation at school, January 2018
- Protecting children from radicalisation: the prevent duty, August 2015

It reflects existing legislation, including but not limited to:

- The Education Act, 1996 (as amended)
- Education and Inspections Act, 2006
- Equality Act, 2010

In addition, it reflects the Education Act, 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.



Roles and Responsibilities

The governing body

The governing body has overall responsibility for monitoring this policy and holding the headteachers to account for its implementation.

The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (ICT Acceptable Use policy)

The headteachers

The headteachers are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead (DSL)

Details of the school's DSL and deputies are set out in our Safeguarding and Child protection policy.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteachers in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, Technology subject leader, ICT service provider (ICON) and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety in liaison with the Technology subject leader
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing body

The ICT service provider - ICON

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school. We use Schools' Broadband whose filtering system is Netsweeper
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Securely locating all servers, wireless systems and cabling and restricting physical access
- Providing users with clearly defined access rights to school technical systems and devices
- Providing all users with a username and secure password. Users are responsible for the security of their username and password.
- Providing the headteachers with the "master/administrator" systems passwords
- Ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

All staff and volunteers

All staff, including contractors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are reported and logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet, where relevant and appropriate

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot Topics - Childnet International
- Parent Factsheet - Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Filtering and Monitoring

Frank Wise School uses School's Broadband, which has Netsweeper as its filtering system. School's Broadband has filed a submission with the UK Safety Internet Centre, the details of which are held by both ICON and the DSL at school. ICON and the DSL are satisfied that the filtering criteria are robust and detailed and align with *Keeping Children Safe in Education.* The balance between keeping everyone safe and over blocking is taken into consideration and ICON and the DSL are clear that content which is required for educational purposes is accessible to all. Please see *Filtering Provider Checklist Response* which details how the system manages specific content and meets core principles, including that of overblocking.

ICON and the DSL meet every half term to review any incidences of overblocking and any Prevent alerts which have been received to agree what actions are required, be that training for staff, learning for pupils, liaison with School's Broadband or potentially a referral to Channel.

It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision.

Education and Training

Pupils

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities provided in the following ways:

- A planned online safety curriculum should be provided as part of Technology / PHSE / PSD lessons and should be regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices and should be explicit in that modelling, for example when checking emails
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit

Risks that pupils will learn about fall into four broad categories:

- **Contact** - Being contacted online by those that wish to bully, groom or inflict harm.
- **Conduct** - An awareness of the impact that any online activity can have on both the user and other people, and the digital footprint that is created on the internet.
- **Content** - Age-inappropriate or unreliable content that may be hurtful or harmful. This includes content accessed and viewed via social networks, online games, blogs and websites.

- **Commercialism** - Exposure to inappropriate commercial advertising, marketing schemes or hidden costs.

This policy aims to mitigate these risks and ensure that the Frank Wise School community can remain safe whilst enjoying all the benefits that technology has to offer.

Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Frank Wise School online safety policy and acceptable use agreements. This is part of the Generalist Safeguarding training all staff undertake.
- An audit of the online safety training needs of all staff with be carried out periodically and training given in response to that
- Online safety training may also be offered within the CPD section of the monthly staff meetings
- It is expected that some staff will identify online safety as a training need within the Appraisal process
- The Technology subject leader will receive regular updates through attendance at external training events and/or by reviewing guidance documents released by relevant organisations
- This online safety policy and its updates will be presented to and discussed by staff in staff or team meetings and training sessions
- The Technology subject leader and DSL with liaise to provide advice, guidance and/or training to individuals as required

Families

Parents and carers may have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/carers evenings/sessions
- Reference to the relevant web sites/publications

Governing Body

The governing body should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in health and safety or safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation.
- Participation in school training/information sessions for staff or parents

Use of digital images and videos

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, families and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, social media or local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use as this is not covered by the Data Protection Act. To respect everyone's privacy and in some cases protection, these images should not be published nor made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims and must follow school policies concerning the sharing, distribution and publication of those images. Those images must only be taken on school equipment; the personal equipment of staff must never be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected careful and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Cyberbullying

This should be read in conjunction with the following policies:

- Behaviour Management
- Bullying
- Peer-on-Peer Abuse

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the policies named above Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Bring Your Own Devices (BYOD)

School staff are allowed to bring their own devices into school and follow the Acceptable Use of ICT agreement and the Staff Handbook with regards to how and when they can be used.

Except in exceptional circumstances, pupils are not permitted to bring their own devices into school other than communication devices. If a pupil is required to do so, for the purposes of their own safety, then these devices are kept by members of staff throughout the day and returned to that pupil at the end of the school day. This is because those devices are not protected by our robust filtering and monitoring processes.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to cause harm.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should delete the material or retain it as evidence and/ or report it to the police.

Acceptable Use

All staff, volunteer and governor are expected to read and sign the ICT Acceptable Use policy will specifies conduct in school and out of school with regards to online activity and the use of school technologies.

See ICT Acceptable Use Policy

Data Protection

Frank Wise School has a General Data Protection Regulation (GDPR) policy which is reviewed regularly. It includes a data breach procedure. Staff and governors are given regular updates and guidance on practices they must or should be following.

Responding to Issues of Misuse

Pupil

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, bullying, or peer-on-peer abuse as appropriate. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate. We have a range of templates we may use to record the event and subsequent action. These include:

- Online Incident Recording Form
- Checklist of Bullying Behaviours
- Online Safety Plan

Staff

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Handbook and staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

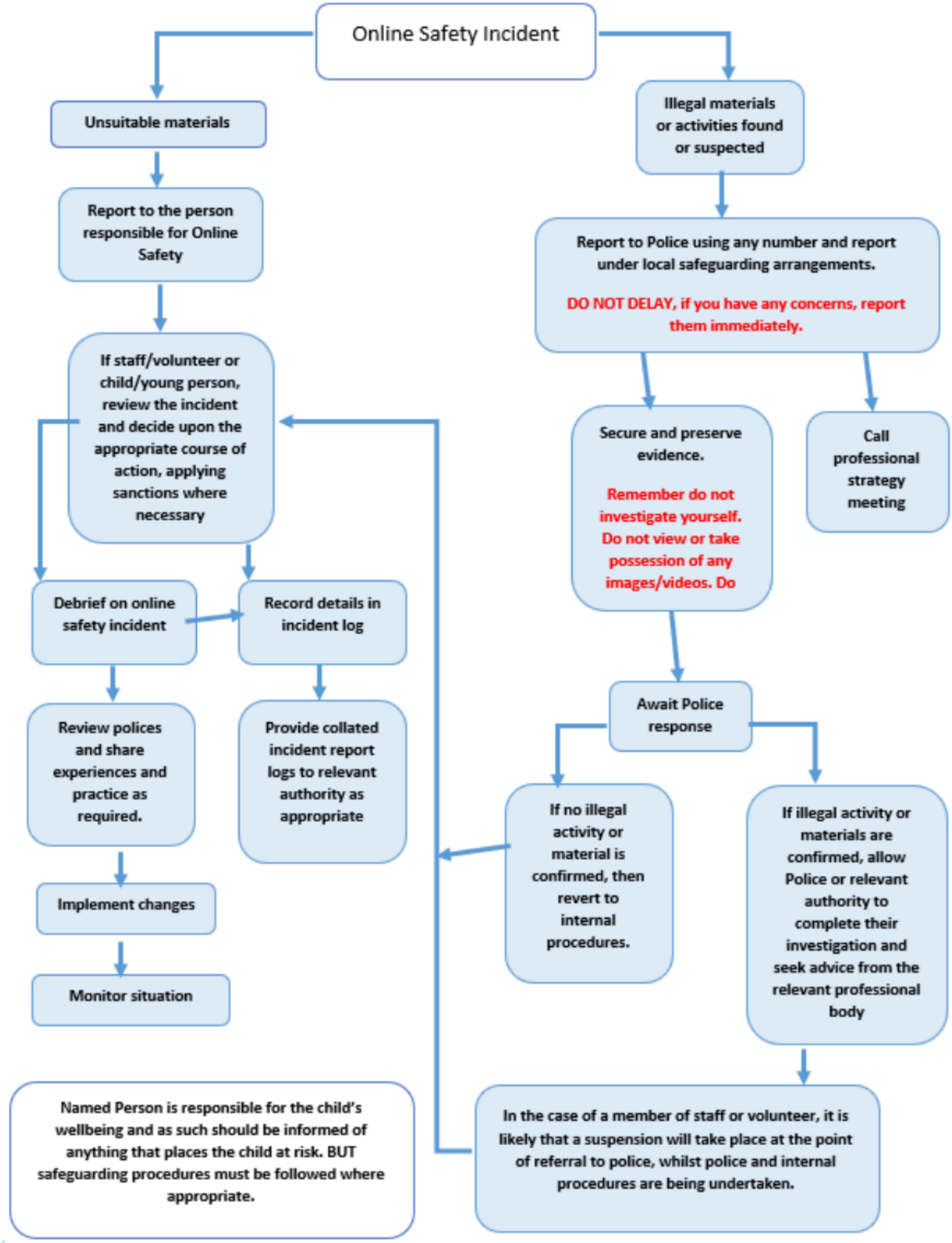
Monitoring Arrangements

The DSL will monitor behaviour and safeguarding issues related to online safety which have been recorded on CPOMS.

This policy will be reviewed annually.

Reviewed by: Lara Hughes **Date:** December 2023

Approved by Governors: Shirley Gelleburn **Date:**


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Online Content / Commercialism Incident

Content / Commercialism (delete as appropriate)			
Name of pupil		Name of staff member	
Date of incident		Date notified of incident	
Was the pupil being monitored at the time?		Has the pupil signed the *Acceptable Use of ICT policy?*	
If the answer to either of the above is NO, then please state why.			
Describe the Incident			
What is the perceived risk of harm?			
Are there any immediate mitigating factors (to support the pupils or to reduce the risk of future incidents?)			
What action will be taken Add / Remove suggestions			

Safety Plan

Safety Plan for					
Completed by		Date			
What is the purpose of the Safety Plan?					
Have other incident forms been completed? If YES, then please attach					
What devices does the pupil have access to?					
Home		School			
Do they have appropriate privacy and filtering settings applied?		Home		School	
Does the pupil understand what they can use devices for?					
Pupil response (What do they understand - in their own words)					
Does the pupil know what they cannot use devices for?					
Pupil response (What do they understand - in their own words)					
Does the pupil understand what risks are associated with an online presence?					
Pupil response (What do they understand - in their own words)					
Does the pupil know who they can talk to if they are worried about something that happens online?					
Pupil response (What do they understand - in their own words)					
Actions				Named Person	Deadline
Pupil signature				Date	
Family signature				Date	
Staff signature				Date	