Online Safety POLICY

Contents

Introduction and Overview

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Thomson House School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Thomson House School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.
- uphold all children's right to privacy and right to protection from violence, abuse and neglect (Article 16 and 19 of the UNCRC).

Who does the policy apply to?

This policy applies to all members of Thomson House School community (including staff, pupils, volunteers, parents / carers, visitors, student teachers and community users) who have access to and are users of school ICT systems, both in and out of Thomson House School.

The Education and Inspections Act 2006 empowers Head Teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school, but is linked to others in the school.

The school will deal with such incidents within this policy and the THS Behaviour Policy and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place both in and out of school.

Role	Key Responsibilities
Headteacher - Jackie Sanders	• Has a duty of care for ensuring the safety (including online safety) of members of the school community. • takes overall responsibility for online safety provision • takes overall responsibility for data and data security. • ensures the school uses an approved, filtered Internet Service, which complies with current statutory requirements. • is responsible for ensuring that the Online Safety Lead and other staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant. • is aware of procedures to be followed in the event of a serious online safety incident. • receives regular monitoring reports from the DSL/Online Safety Lead.
Designated Safeguarding Lead - Ros Williams	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents. • promotes an awareness and commitment to online safety throughout the school community. • ensures that online safety education is embedded across the curriculum. • communicates regularly with SLT and the designated Safeguarding LAC member to discuss current issues, review incidents logged on CPOMS • monitors online safety incidents recorded on CPOMS. • ensures appropriate filtering and monitoring systems are in place, as laid out in Keeping Children Safe in Education 2024. • ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident. • facilitates training and advice for all staff and Governors on a regular basis (at least annually).

Role	Key Responsibilities
	• liaises with the Local Authority and relevant agencies. • liaises with school technical support staff IT technicians. • is regularly updated on online safety issues and legislation, and is aware of the potential for serious child protection issues to arise from: – sharing of personal data – access to illegal / inappropriate materials – inappropriate online contact with adults / strangers – potential or actual incidents of grooming – cyber-bullying and use of social media
Online safety LAC member – Michael Parslow Designated Safeguarding LAC member – Heather Locke	• ensures that the school follows all current online safety advice to keep the children and staff safe. • approves the Online Safety Policy and reviews the effectiveness of the policy. This will be carried out by the Education Committee receiving regular information about online safety incidents and monitoring reports. • a member of the Governing Body takes on the role of Online Safety Governor. • supports the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the Online Safety Governor will include: – regular review with the Online Safety Lead / DSL – regular monitoring of online safety incident logs – reporting to relevant Governors/ Education Committee
Computing Curriculum Leader - Samantha Stevens	• oversees the delivery of the online safety element of the Computing curriculum. • liaises with the Online Safety Lead / DSL regularly.
School IT Support - Click On IT	• ensures that the school's technical infrastructure is secure and is not open to misuse or malicious attack. • ensures that the school meets required online safety technical requirements, including for filtering and monitoring. • reports any online safety related issues that arises, to the Online Safety Lead/DSL.

Role	Key Responsibilities
	• ensures that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed. • ensures that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date. • ensures the security of the school ICT system. • ensures that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • that he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • that the use of the VLE is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Lead / DSL for action. • ensures appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • keeps up-to-date documentation of the school's online security and technical procedures.
Data Protection Officer - Paul Hepworth	• ensures that all data held on pupils on the school office machines have appropriate access controls in place.
Class Teachers	• embed online safety issues in all aspects of the curriculum and other school activities. • supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant). • ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws and plagiarism.

Role	Key Responsibilities
All staff - including peripatetic teachers, volunteers and any other adults in school	• read, understand and help promote the school's online safety policies and online safety guidance. • read, understand, sign and adhere to the school staff Acceptable Use Policy (AUP). • are aware of online safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices. • report any suspected misuse or problem to the DSL. • maintains an awareness of current online safety issues and guidance e.g. through CPD. • model safe, responsible and professional behaviours in their own use of technology. • ensure that any digital communications with pupils should be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• read, understand, sign and adhere to the Pupil Acceptable Use Policies – Upper School and Lower School • understand the importance of reporting abuse, misuse or access to inappropriate materials. • know what action to take if they or someone they know feels worried or vulnerable when using online technology. • know and understand school policy on the use of mobile phones, digital cameras and handheld devices. • know and understand school policy on the taking / use of images and on cyber-bullying. • understand the importance of adopting good online safety practice when using digital technologies out of school and understand that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school • take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home. • help the school in the creation/ review of online safety policies.

Role	Key Responsibilities
Parents/carers	• support the school in promoting online safety which includes the pupils' use of the Internet, photographic and video images. • read, understand and promote the school Pupil Acceptable Use Agreement with their children. • Read, understand and sign the Parent Acceptable Use Agreement. • consult with the school if they have any concerns about their children's use of technology.

Education - Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PHSE/other lessons and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities.
- 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. N.B. additional duties for

schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools to ensure that children are safe from terrorist and extremist material on the internet. See The THS Preventing Extremism Policy.

- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents

Many parents and carers have only 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, Google Classrooms
- High profile events/campaigns e.g. Safer Internet Day

Communication:
The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website, VLE (for staff) and Google Classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to staff at the start of each academic year
- Acceptable use agreements to be issued to parents at the start of each academic year
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school, Click On IT nor Achieving For Children can accept liability for material accessed, or any consequences of Internet access.
- Our DSL acts as first point of contact for any complaint about pupil misuse. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
    - interview/counselling by teacher / Deputy Headteacher / Online Safety Leader / Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period;
    - referral to LA / Police.

Password policy:
The school makes it clear that staff and pupils must always keep their passwords private, must not share them with others and must not leave them where others can find them.

- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private
- We require staff to use strong passwords which are changed regularly
- Staff access to the schools' management information system is controlled through a separate password for data security purposes
- We provide pupils with an individual network log-in username. From Year 4 they are also expected to use a personal password

E-mail
The school

- Provides staff with an email account for their professional use and makes clear personal email should be through a separate account
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

The School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to the admin team
- The school web site complies with the statutory DfE guidelines for publications
- The point of contact on the web site is the school address, telephone number and a general email contact address - office@thomsonhouseschool.org
- Photographs of children published on the website do not have full names attached
- Will not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- Will not use embedded geodata in respect of stored images.

Virtual Learning Environment (VLE)

- Uploading of information on the school's VLE is shared between different staff members according to their responsibilities e.g. all teachers upload information in their year group areas
- Photographs and videos uploaded to the school's VLE will only be accessible by members of the school staff.

Social Media

- No member of staff at THS will link / message / follow a pupil's account
- No reference should be made in social media to students / pupils, parents / carers or school staff
- Staff will not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or Achieving for Children
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

The school

- Predominantly uses Google Meet for video conferencing involving the pupils
- Only uses Zoom for video conferencing when additional security is added
- Only uses approved or checked webcam sites.

CCTV

The school has CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (*retained by the Support Provider for 14 days*), without permission except where disclosed to the Police as part of a criminal investigation.

Signage clearly indicates that CCTV is present and recording on school premises.

THS uses specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Data security: Management Information System access and Data transfer

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school will ensure that:

- it has a Data Protection Policy.
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.

Strategic and operational practices

At this school:

- The Data Protection Officer is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised – the Headteacher and DPO.
- All staff are DBS checked and records are held in one central record in a password protected spreadsheet.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

- staff,
- governors,
- pupils
- parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.

- We follow Achieving for Children guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in Achieving for Children or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School admin staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical Solutions

- Staff have a password protected secure area(s) on the network to store sensitive documents or photographs.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the DfE S2S site to securely transfer CTF pupil data files to other schools.
- We use the Pan-London Admissions system (based on USO FX) to transfer admissions data.
- We use Egress to transfer other data to schools in London, such as references, reports of children.
- We use CPOMS to record safeguarding concerns.
- We use Senso to monitor staff and pupil computer usage.
- We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- All servers are in lockable locations and managed by DBS-checked staff.
- Portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through a secure procedure.

- Paper based sensitive information is collected by secure data disposal service.

Equipment and Digital Content

Pupils - Personal mobile phones and mobile devices

The school forbids mobile phones of pupils in school.

If a pupil breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers at the end of the day.

If a pupil needs to contact his or her parents or carers, the office will do it. Parents are advised to call the school office if they need to contact their child.

Staff - Personal mobile phones and mobile devices

Mobile phones brought into school are entirely at the staff member's, parent's, or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.

Staff members may use their phones during their break times but not in lesson times. All visitors are requested to keep their phones on silent.

In certain situations, such as during school trips, staff may need to use their mobile phones to communicate with other staff members, parents, or carers. In these instances, staff will ensure that their mobile phone usage complies with the guidelines outlined in the Staff Code of Conduct.

The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher and Deputy Headteachers. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary. Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.

The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or handheld devices may be searched at any time as part of routine monitoring.

If a staff member is expecting a personal call, they may leave their phone with the school office to answer on their behalf or seek specific permissions to use their phone at other than their break times.

Mobile phones and personally owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. If members of staff have an educational reason to allow children to use mobile phones or a personally owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.

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

If a member of staff breaches the school policy, then disciplinary action may be taken.

Mobile phones and personally owned devices are not permitted to be used in certain areas within the school site, e.g., changing rooms and toilets.

The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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. 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/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 such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/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, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not 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 carefully and will comply with good practice guidance on the use of such images.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Filtering & Monitoring

- The DSL is responsible for filtering and monitoring.
- Appropriate filtering and monitoring on school devices and networks is in place. The effectiveness of these systems are reviewed regularly.
- Filtering systems block harmful and inappropriate content without unreasonably impacting teaching and learning.
- All staff are aware of filtering and monitoring, and have received training to ensure an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Appendices:

1. Responding to incidents of misuse flow chart
2. Links to helpful organisations and documents

Review and Monitoring

The online safety Policy will be shared with staff annually. Senior Leaders are responsible for monitoring compliance with the policy.

Agreed by: Senior Leadership Team

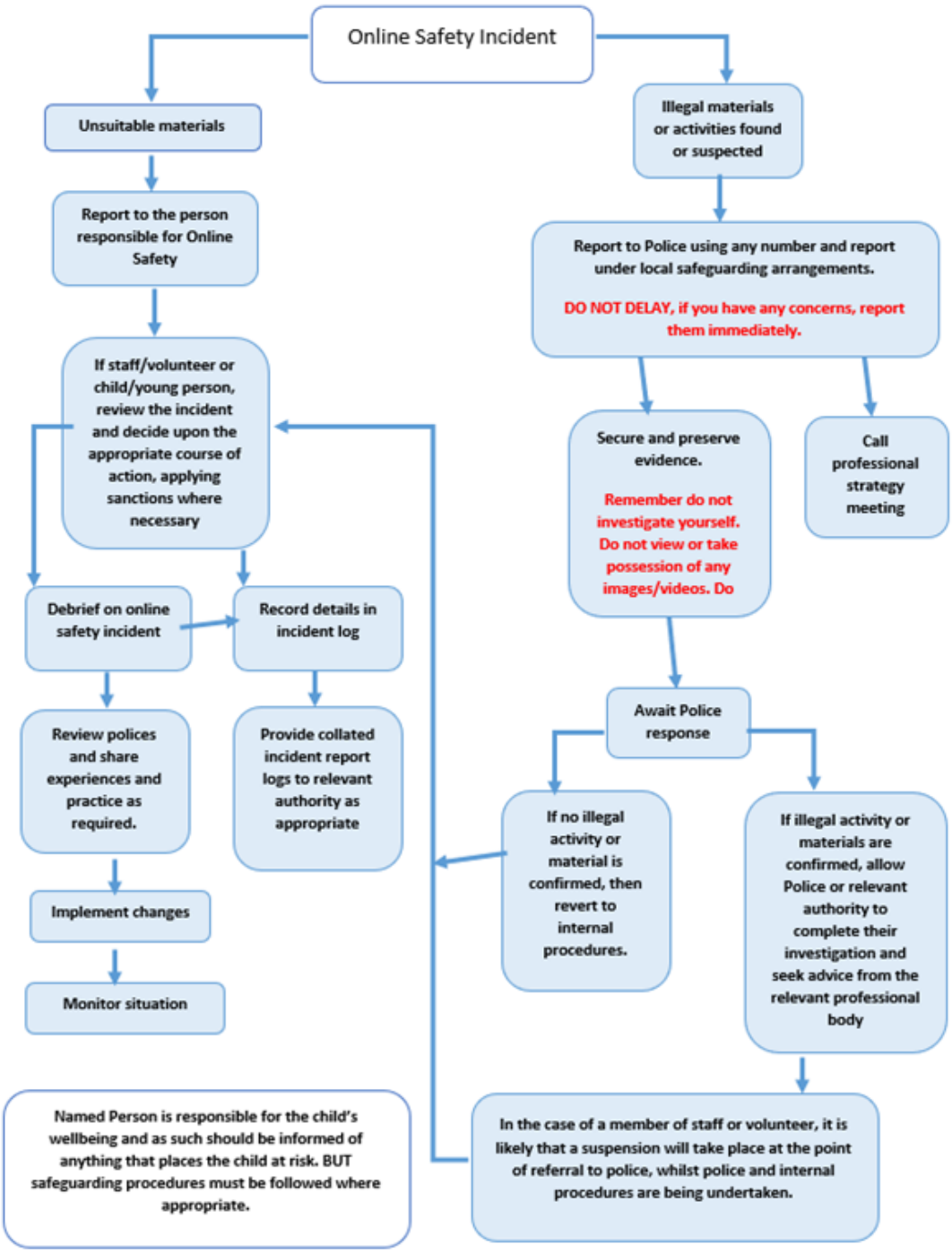
Date: Feb 2025

Review Cycle: Annual

Next Review Date: Feb 2026

Responding to Incidents of misuse – flow chart

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Childnet – http://www.childnet-int.org/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

Revenge Porn Helpline - https://revengepornhelpline.org.uk/

Internet Watch Foundation - https://www.iwf.org.uk/

Report Harmful Content - https://reportharmfulcontent.com/

CEOP - http://ceop.police.uk/

ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources

Kent – Online Safety Resources page

INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

Netsmartz - http://www.netsmartz.org/

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/

SELMA – Hacking Hate - https://selma.swgfl.co.uk

Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/

Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388

DfE - Cyberbullying guidance -

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:
http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit

Childnet – Project deSHAME – Online Sexual Harrassment

UKSIC – Sexting Resources

Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm

Ditch the Label – Online Bullying Charity

Diana Award – Anti-Bullying Campaign

Data Protection
360data - free questionnaire and data protection self review tool

ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act

IRMS - Records Management Toolkit for Schools

NHS - Caldicott Principles (information that must be released)

ICO Guidance on taking photos in schools

Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education

DfE - Safer Working Practice for Adults who Work with Children and Young People

Childnet – School Pack for Online Safety Awareness

UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support
UKSIC – Appropriate Filtering and Monitoring

SWGfL Safety & Security Resources

Somerset - Questions for Technical Support

NCA – Guide to the Computer Misuse Act

NEN – Advice and Guidance Notes

Working with parents and carers

Online Safety BOOST Presentations - parent's presentation

Vodafone Digital Parents Magazine

Childnet Webpages for Parents & Carers

Get Safe Online - resources for parents

Teach Today - resources for parents workshops/education

Internet Matters

Prevent

Prevent Duty Guidance

Prevent for schools – teaching resources

NCA – Cyber Prevent

Childnet – Trust Me

Research

Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework