St. Andrew's CE Primary School

Online Safety Policy

Approved by:	Teaching & Learning Committee
Last reviewed on:	November 2025
Next review due by:	Autumn 2026

Introduction

Key people / dates

Designated Safeguarding Lead (DSL) team	Kim Murdock/ Sarah Chambers
Online Safety Lead	Dan Buchanan
Computing Lead	Dan Buchanan
Online-safety / safeguarding link governor	Sylvie Ruck
PSHE/RSE lead	Laura Ovnik
Data Protection Officer	Data Protection Education Ltd Registered office: 1 Saltmore Farm, New Inn Rd, Hinxworth, Baldock, SG7 5EZ Telephone: 0800 0862018 Email: dpo@dataprotection.education
Business Manager	Leanne Phair
Network manager / other technical support	Kevin Astle/ Rab Atmani/ Andy Smith BHCC ICTSTS
Date this policy was reviewed and by whom	**November 2025** Teaching and Learning Committee
Date of next review and by whom	**Autumn 2026** Teaching and Learning Committee

What is this 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 2025 (KCSIE), 'Teaching Online Safety in Schools' and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. Although many aspects will be informed by legislation and regulations, we also involve staff, governors, pupils and parents/carers in writing and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

KCSIE makes it clear that "the designated safeguarding lead (DSL) should take lead responsibility for safeguarding and child protection (including online safety)." The Computing Subject Lead and PSHE Subject Lead work alongside the DSL in promoting and ensuring online safety in school.

What are the main online safety risks today?

Online safety risks are traditionally categorised as one of the 4 Cs: Content, Contact, Conduct, Commerce (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, e.g. fake news, up skirting and sticky design. To keep yourself updated with prominent new and emerging trends, follow websites such as parents/carers/carerszone.org.uk safety-net.org.uk and www.childnet.com .

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It will 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/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, pupils and parents/carers/carers.
- 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 all classrooms and by internet usage devices that children access.
- Reviews of this online safety policy will include input from staff, pupils and other stakeholders, helping to ensure further engagement.

Contents

Overview

Aims

This policy aims to:

- Set out expectations for all St Andrew's CE Primary School community members' online behaviour, attitudes and activities and use of digital technology
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, 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, to survive and thrive online
- 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)

Scope

This policy applies to all members of the St Andrew's CE Primary School community (including staff, governors, volunteers, contractors, pupils, parents/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 – Sophie Thomas

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- 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 for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- 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
- 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 carry out internal technical online safety procedures
- Ensure governors are regularly updated 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: Kim Murdock/Sarah Chambers/ Dan Buchanan

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

- "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety)." Aspects of online safety are delegated to the Online Safety Lead.
- Where the Online Safety Lead 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 the local authority Paul Platts and work with other agencies in line with Working together to safeguard children"
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Work with the headteacher, DPO and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data protection processes support careful and legal sharing of information
- Stay up to date with the latest trends in online safety e.g. NSPCC, Safety Net, Parents/carers Zone
- 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
- Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life
- Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents/carers, who are often appreciative of school support in this area, but also including hard-to-reach parents/carers
- Liaise with school technical, pastoral, and support staff as appropriate
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues, review incident logs.
- 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
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this).
- Ensure the 2021 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:
    - 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 C (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more

Governing Body, led by Online Safety / Safeguarding Link Governor – Chris Simmons

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

- 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 (October 2022)
- "Ensure an appropriate **senior member** of staff, from the school or college 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/carers and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the Online Safety Lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online safety lead 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 GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Check all school staff have read Part 1 of KCSIE; SLT and all working directly with children have read Annex 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. The training should be regularly updated in line with advice from the local authority and other relevant agencies integrated, aligned and considered as part of the overarching safeguarding approach."
- "Ensure appropriate filters and appropriate monitoring systems are in place but 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. Consider a whole school or college approach to online safety with a clear policy on the use of mobile technology." NB – refer to Teaching Online Safety in Schools' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World' to support a whole-school approach.

All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are; see the list at the beginning of this policy.
- 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 (using CPOMS) 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 AUP and code of conduct.

- 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, 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 (devices, the internet, new technology such as augmented reality, AI etc.) in school or setting as homework tasks, encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.
- To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), 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.
- Prepare and check all online source and resources before using within the classroom, including the viewing of any video footage.
- Encourage pupils to follow their acceptable use policy, remind them about it and enforce school sanctions
- Notify the DSL/OSL 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 most likely to see or overhear online safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom – let the DSL/OSL know
- Receive regular updates from the DSL/OSL and have a healthy curiosity for online safety issues – you may find it useful to read at least the headline statistics and conclusions from the LGfL DigiSafe pupil survey of 40,000 pupils
- 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 Lead – Laura Ovnik

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the PSHE / 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/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within PSHE.

Computing Lead – Dan Buchanan

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
- Work closely with the DSL/PSHE leads 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
- Work with the headteacher to ensure the school website meets statutory DfE requirements.

Subject Leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, 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/OSL 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 (where appropriate/relevant)

Network Manager/technician – Kevin Astle/Rab Atmani/Andy Smith

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Work closely with the designated safeguarding lead / online safety lead / 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 (especially in terms of access to personal and sensitive records / data and to systems such as YouTube mode, web filtering settings, sharing permissions for files on cloud platforms etc.)
- 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 (see appendices for website audit document) Liaise with HT/DSL/OSL.

Data Protection Officer (DPO – Data Protection Education Ltd.) Leanne Phair

Key responsibilities:

- NB – this document is not for general data-protection guidance;
- Be aware 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' (February 2023), especially this quote from the latter document:
  "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 parents/carers/carers/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."*
- 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 (by governors)

Volunteers and contractors

Key responsibilities:

- Read, understand, sign and adhere to an Acceptable Use Policy (AUP) if using any school related technology.
- Report any concerns, no matter how small, to the designated safety lead / online safety lead.
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the pupil Acceptable Use Policy and review this annually
- 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
- 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
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems

Parents/carers

Key responsibilities:

- Read and promote the school's parents/carers 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/carers.

External groups including parents/carers/carers associations – e.g. PTA, any after school clubs including coding, Dance Teacher, Gymnastics Coach

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy (AUP) prior to using technology or the internet within school.
- 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/carers/carers

Education and curriculum

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

- Personal, social, health and economic education (PSHE)
- Relationships education, relationships and sex education (RSE) and health education
- Computing
- Citizenship

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/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 (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 and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. Saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents/carers. Also see posters.lgfl.net and reporting.lgfl.net.

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

Parents/carers involvement

- Parents/carers' attention will be drawn to the school's Online Safety page via newsletters or weekly information.
- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents/carers will be encouraged. This may include parents/carers evenings with demonstrations and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents/carers

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, PSHE, RSE 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 online safety lead / 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 concerns are detailed in the Anti-bullying Policy and the Behaviour Policy (https://www.st-andrews.brighton-hove.sch.uk/governance-policies/school-policies.)

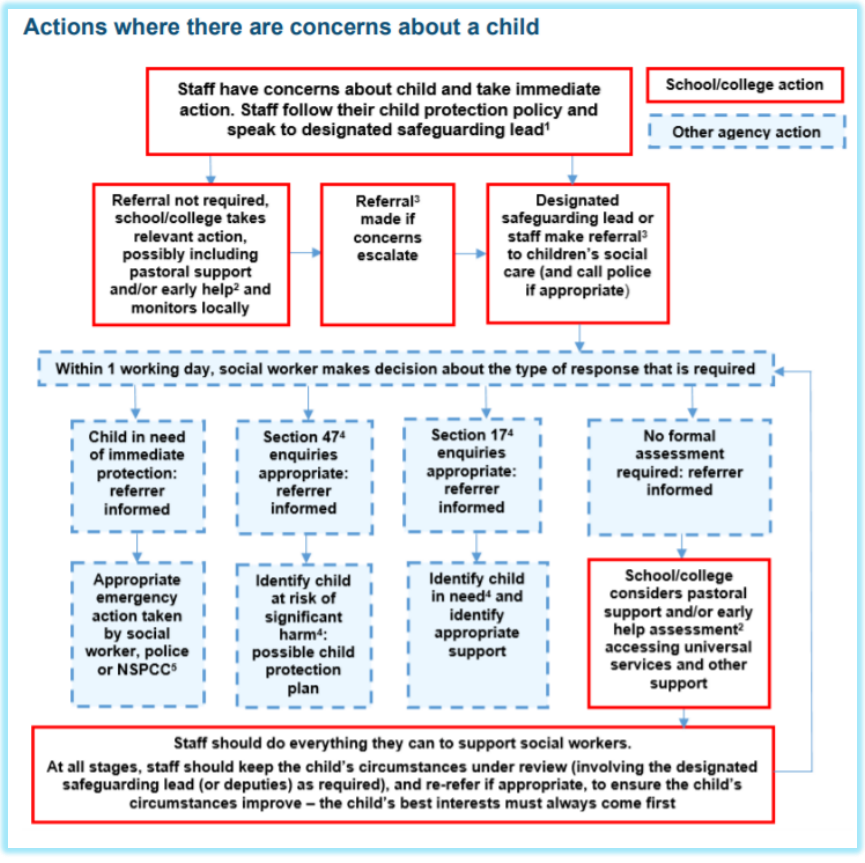
This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school, and that those from outside school will continue to impact on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson.

Any concern/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 and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline , phone 0800 028 0285 or email help@nspcc.org.uk

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

This flow chart, taken from 'Keeping Children Safe in Education', is used to guide processes.



Bullying

Online bullying should be treated like any other form of bullying and the school anti-bullying policy should be followed for online bullying, which may also be referred to as cyberbullying.

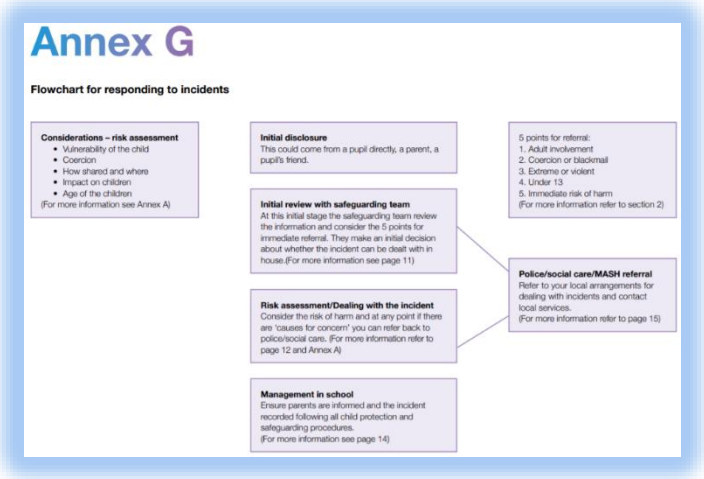
It is important **not** to treat online bullying separately to offline bullying and to recognise that bullying will often have both online and offline elements.

Sexting

Any incidences of sexting should be referred directly to the DSL who will in turn use the full guidance document Sexting in Schools and Colleges to decide next steps.

This flow chart is taken from page 47 of Sexting in Schools and Colleges.

See



https://www.gov.uk/government/publications/sexting-in-schools-and-colleges

Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and is 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 are defined in the relevant Acceptable Use Policies as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

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

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or, if applicable, 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 St Andrews CE Primary School community. These are also governed by school Acceptable Use Policies. Breaches will be dealt with in line with the school behaviour policy (for pupils) or code of conduct (for staff).

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

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

Data protection and data security

"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 parents/carers 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/carers 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
- Remote Access provided by Brighton & Hove City Council
- Office365 – OneDrive secure cloud storage
- Egress Encrypted email
- Send IT
- CPOMS

The headteacher, data protection officer and governor's 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, and 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] not be able to access harmful or inappropriate material, but at the same time 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."

At this school, the internet connection is provided by Brighton & Hove City Council ICT Schools & Traded Services. This means we have a dedicated and secure connection that is protected with firewalls and multiple layers of security, including a web filtering system called Smoothwall, which is designed specifically to protect children in schools. You can read more about appropriate filtering and monitoring systems on the UK Safer Internet Centre's website.

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

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

At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. At Key Stage 2 this broadens to allow for independent but supervised Internet use.

As well as children being physically monitored, all users of the internet in school may be monitored via the Smoothwall filtering system and their browsing habits logged for reference if needed. Daily reports and instant alerts are sent to school for review.

Electronic communications

Please read this section alongside the Social Media section of this policy and 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

- Only school staff and governors are able to communicate via the school e-mail system.
- Staff use Office365 system for all school emails. This system is fully auditable, trackable and managed by BHCC (Office365). This is for the mutual protection and privacy of all staff, pupils and parents/carers, as well as to support data protection.

General principles for email use are as follows:

- Email via the school office address is the only means of electronic communication to be used between staff and parents/carers (in both directions).
- Office 365 and LAN messenger are the primary means of electronic communication to be used between members of staff. Use of different platforms (e.g. personal texts, WhatsApp etc.) must be approved in advance by the headteacher. 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) to the headteacher (if by a staff member) or to the Chair of Governors (if by the headteacher).
- The school email system only be used for official school business; if used for other purposes 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, encrypted email via Office365 and Egress must be used.
    - Internally, staff should use the school network and OneDrive, including when working from home. Remote access may also be available for a few key members of staff, such as the Business Manager or headteacher.
- 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.
- Staff are **NOT** allowed to use the **email system** for personal use and 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.

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 has been the day-to-day responsibility of updating the content of the website to Andy Smith. The site is managed by / hosted by Webanywhere.

The DfE has determined information which must be available on a school website. The school regularly audits the website to ensure that these requirements are met. https://www.gov.uk/guidance/what-maintained-schools-must-publish-online

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

- Schools have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission. If in doubt, check with the school business manager.
- 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

Many schools are recognising the benefits of cloud computing platforms, not just for cost savings but to enhance teaching and learning.

This school adheres to the principles of the DfE document 'Cloud computing services: guidance for school leaders, school staff and governing bodies'. Microsoft Office 365 cloud platform is used at this school.

As more and more systems move to the cloud, it becomes easier to share and access data. It is important to consider data protection before adopting a cloud platform or service – see our Data Protection policy here.

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/or the network manager will regularly review system documents and procedures both during and after their implementation.

The following principles apply:

- Privacy statements inform parents/carers and children (13+) when and what sort of data is stored in the cloud.
- 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 parents/carers permission is sought if necessary.
- 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 will be clearly marked as such as part of our ongoing updates to the school network.
- Pupil images/videos are only made public with parents/carers permission
- Only school-approved platforms are used by pupils or staff to store pupil work.

Digital images and video

When a pupil joins the school, parents/carers are asked if they give consent for their child's image to be captured in photographs or videos, for what purpose (beyond internal assessment, which does not require express consent) and for how long (currently 7 years).

Whenever a photo or video is taken/made of a child, the member of staff taking it will check the latest list held by the office 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, the staff code of conduct and the school's Acceptable Use Policy, which states that no member of staff will use their personal phone or other equipment to capture photos or videos of pupils.

Photos are stored on the school network and other platforms authorised by the headteacher (e.g. blogs for residential trips) in line with the retention schedule of the school Data Protection Policy.

Staff and parents/carers are reminded regularly 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.

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/carers 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

St Andrew's Social Media presence

Here at St Andrew's we work 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/carers will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online. Negative coverage almost always causes some level of disruption and possibly damage to the reputation of the school.

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.

Staff, pupils' and parents/carers' social media 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/carers, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community have access to, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parents/carers chats, pages or groups. Naming a child too on social media is totally inappropriate and a potential safeguarding issue.

If parents/carers have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure here should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents/carers, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13, but the school sometimes deals with issues arising on social media with pupils under the age of 13. We ask parents/carers to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

The school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents/carers can best support this by talking to their children about the apps, sites and games they use, 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 introduce the Children's Commission Digital 5 A Day.

School Comms and Email are the official electronic communication channels between parents/carers and the school.

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 such public pupil social media/networking accounts.

-Exceptions may be made, e.g. for pre-existing family links, but these must be approved by the headteacher and should be declared upon entry of the pupil or staff member to the school).

-Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the headteacher (if by a staff member) or to the Chair of Governors (if by the headteacher).

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. They should never discuss the school or its stakeholders on social media and be careful that their personal opinions might not be attributed to the school bringing it into disrepute. Staff are also reminded to not state their school name on their social media pages.

Device usage

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 electronic communication devices (e.g. mobile phones, smart watches etc.) in to school for use outside school hours. During the school day all electronic communication devices must remain turned off at all times and handed into the class teacher for safekeeping. Sanctions in line with the Behaviour Policy will be given for attempts to use a phone in lessons without permission (level 3) or to take illicit photographs or videos (level 4). Important messages and phone calls to or from parents/carers can be made at the school office, which will also pass on messages from parents/carers to pupils in emergencies.
- **All staff who work directly with children** should leave their mobile phones on silent, out of sight and out of reach e.g. in a cupboard or locked drawer. Phones should only be used in private staff areas during school hours, such as the PPA room, staffroom and office areas. Also see the sections on 'Digital images and video' and Data protection and data security' of this policy. Child/staff data should never be downloaded onto a private phone. If a staff member is expecting an important personal call when teaching or otherwise on duty, they may leave their phone with the school office to answer on their behalf or ask for the message to be left with the school office.
- **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. photos of equipment or buildings by contractors), permission of the headteacher should be sought in the presence of a member of staff (the headteacher may choose to delegate this).
- **Parents/carers** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing children other than their own. When at school events, please refer to the Digital Images and Video section of this document, our Photographic and Filming Policy Statement and our photo consent form which is completed when children join the school. Parents/carers are asked to communicate with their children only via the school office during the school day.

Network / internet access on school devices

The school Wi-Fi network is solely for school-related internet use using school owned devices such as iPads. All such use is monitored.

Trips / events away from school

For school trips/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/carers. Any deviation from this policy (e.g. 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 parents/carers or pupil accessing a teacher's private phone number.

Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/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 also be aware of sexting issues detailed above which should be reported directly to the DSL).

Appendices

Sources referred to in this policy and used at this school.

School Policies	
https://www.st-andrews.brighton-hove.sch.uk/governance-policies/school-policies	
Advice and guidance for schools	
Keeping Children Safe in Education (KCSIE), see p 96 Annex C	
Teaching Online Safety in Schools ; DfE guidance for existing curriculum requirements; next review spring 2021	
Relationships and Sex Education (PDF Sept 2020; reviewed every three years)	
Working together to safeguard children (PDF 2018)	
Education for a Connected World framework for EYFS to 18 (UKCIS) (PDF 2020)	
sexual violence and harassment (PDF 2018)	
www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people	
www.gov.uk/guidance/what-maintained-schools-must-publish-online	
Cloud computing services: guidance for school leaders, school staff and governing bodies	
Searching, screening and confiscation: advice for schools	
Data protection: a toolkit for schools (August 2018)	
Online safety in schools and colleges: Questions from the Governing Board (UKCIS June 2020)	
	Professor Tanya Byron's 2008 report
pupil survey of 40,000 pupils by LGfL DigiSafe	
www.iwf.org.uk	Internet Watch Foundation
www.nationalcrimeagency.gov.uk	National Crime Agency (NCA)
www.ceop.police.uk/safety-centre/	Child Exploitation and Online Protection
www.virtualglobaltaskforce.com	Virtual Global Taskforce
www.nspcc.org.uk/what-you-can-do/report-abuse/dedicated-helplines/whistleblowing-advice-line	NSPCC Whistleblowing Helpline; phone 0800 028 0285 or email help@nspcc.org.uk
www.saferinternet.org.uk	Specialist helpline for UK schools and colleges.
https://nationalonlinesafety.com/	Advice and resources for parents/carers and schools.
London Grid for Learning e.g. cpd.lgfl.net, saferesources.lgfl.net, posters.lgfl.net, reporting.lgfl.net	
Other resources	
www.childrenscommissioner.gov.uk/our-work/digital/5-a-day	practical online health advice for young people
www.brightonandhovelscb.org.uk	Brighton and Hove Child Safeguarding
https://www.bbc.com/ownit	CBBC OwnIt
www.childline.org.uk	Childline , 0800 1111
www.digitalawarenessuk.com	Digital Awareness UK
www.digizen.org	Digizen (part of Childnet)
https://www.naace.co.uk	National Assoc. for technology in education
www.nen.gov.uk	National Education Network
learning.nspcc.org.uk, www.net-aware.org.uk	NSPCC / Netaware (guide to social networks)
www.pshe-association.org.uk	PSHE curriculum guidance for schools.
www.thinkuknow.co.uk	Think U Know (produced by NCA & CEOP)
parents/carers/carerszone.org.uk	Parents/carers/carers Zone – Digital Parents/carers Magazine Be Internet Legends curriculum resources.
parents/carers/carersinfo.org	Advice from CEOP and Parents/carers/carers Zone
www.safetynetkids.org.uk , www.safety-net.org.uk/	Safety Net
www.childnet.com	Curriculum resources (e.g. Digiduck, Smarty the Penguin, The SMART crew)

www.commonsensemedia.org	Independent reviews, age ratings etc. about all types of media for children and their parents/carers
https://www.internetmatters.org/	Advice for parents/carers/carers