

The Priory CE VA Primary School

Inspiring all to learn, flourish and achieve



Online Safety Policy

Online Safety Policy			
Approval	Board of Governors	Chairman	Sue Solly
Headteacher	Paul Ruffle	Ratified	
Date of last review	April 2021	Date of this review	July 2023
Date of next review	July 2024	Maintenance	Paul Ruffle / Online safety Champion
Key Information Online Safety Champion - Paul Ruffle (NSPCC training) Safeguarding Governor – Dominic Jones Network Manager - TurnITOn			

Important Note: This policy needs to be read in conjunction with the Child Protection Policy and Acceptable Use Policies. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Contents

Contents	2
1. Introduction	4
1.1 Scope	4
1.2 Aims	4
1.3 How will this policy be communicated?	4
2. Roles and responsibilities	5
2.1 Headteacher (and lead DSL)	5
2.2 Online Safety Champion	5
2.3 Governing Body (led by Safeguarding Link Governor)	6
2.4 All staff	6
2.5 Network Manager & Technical Support	7
2.6 Volunteers and contractors (including tutors)	7
2.7 Pupils	8
2.8 Parents/Carers	8
2.9 FPS Facebook Groups	8
3. Education and Training	9
3.1 Curriculum	9
3.2 Pupils	9
3.3 Parents/Carers	9
4. Data protection and data security	10
5. Appropriate filtering and monitoring	10
6. Electronic communications	11
6.1 Email	11
6.2 Video Conferencing	11
7. School website	12
8. Cloud platforms	12
9. Digital images and video	12
10. Social media	13
10.1 The Priory School's Social Media Presence – Twitter and YouTube	13
10.2 Staff, pupils' and parents' Social Media presence	14
11. Device usage (including mobile phones in school)	15
11.1 Personal devices including wearable technology and bring your own device (BYOD)	15
11.2 Network / internet access on school devices	16
11.3 Devices used for trips / events away from school	17

12. Searching and confiscation	17
13. Handling online-safety concerns and incidents	17
13.1 Actions where there are concerns about a child	18
13.2 Sexting	19
13.3 Upskirting	19
13.4 Online Bullying (sometimes referred to as Cyberbullying)	19
13.5 Sexual violence and harassment	20
13.6 Misuse of school technology (devices, systems, networks or platforms)	20
13.7 Illegal Incidents Flowchart and Procedure	20
13.8 Social media incidents	22
13.9 Prevent	22
13.10 Indecent Images and pornography	23
14. Monitoring and evaluation	23
15. Policy Version History	23
Appendix 1 – Recording Form for investigating devices / internet sites	24
Appendix 2 – Reporting Log for Responding to Incidents of Misuse	25
Appendix 3 – Legislation	26
Appendix 4 – Loaned Laptop Indemnity	31
	31

1. Introduction

1.1 Scope

This policy applies to all members of the school (including staff, pupils, governors, volunteers, parents / carers, visitors, community users) who have access to and are users of school IT systems, either on-site or remotely, including our guest wifi network.

1.2 Aims

This policy aims to:

- Set out expectations for all The Priory School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline).
- 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 flourish 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 in their care
 - 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's mission 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 the school's Behaviour Policy and Child Protection Policy).

1.3 How will this policy be communicated?

- Posted on the school website
- Available on the school's 'Priory Education' G Drive in the Computing Folder
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers & the core policy Autumn reading pack)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers.
- AUPs issued to whole school community, on entry to the school (e.g. *as part of the Reception Welcome Pack*), with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- AUPs are displayed in appropriate classrooms/corridors (not just in Computing corridors/classrooms)

2. Roles and responsibilities

This school is a community and all members have a duty to behave respectfully online and offline. It is everyone's responsibility to 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.

2.1 Headteacher (and lead DSL)

Key responsibilities:

- Foster a culture of safeguarding where online safety (including remote learning safety) is fully integrated into whole-school safeguarding
- Ensure that policies and procedures are followed by all staff, and that all have received appropriate training
- Liaise with the Online Safety Champion/DSL's to work together on any online-safety issues which might arise and receive regular updates on 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 IT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- 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 assessing the risk of children being radicalised (the Prevent Strategy)
- 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
- Ensure the 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 all forms of bullying
- Facilitate training and advice for all staff, including supply teachers:
 - all staff must read KCSIE Part 1 and all those working with children Annex A
 - it would also be advisable for all staff to be aware of Annex C (online safety)

2.2 Online Safety Champion

Key responsibilities

- Work with the HT and technical staff to review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (complete the annual **360safe audit**)
- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use

- Review and update this policy, other online safety documents (e.g. Acceptable Use Policies) and submit for review to the governors/trustees
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework '*Education for a Connected World – 2020 edition*') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents – materials at parentsafe.lgfl.net
- Communicate regularly with SLT and the designated safeguarding and online safety governor/Standards Committee to discuss current issues (anonymised), review incident logs (see **Appendix 2**) and discuss how filtering and monitoring work and have been functioning/helping.
- 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 (CPOMs).

2.3 Governing Body (led by Safeguarding Link Governor)

Key responsibilities

- 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](#) and checking the **annual 360Safe audit**.
- Ask about how the school has reviewed protections for **pupils in the home** (including when with online tutors) and **remote-learning** procedures, rules and safeguards
- Support the school in encouraging parents and the wider community to become engaged in online safety activities
- Have regular strategic reviews with the online-safety Champion or lead DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- 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

2.4 All staff

Key responsibilities:

- Understand that online safety is a core part of safeguarding and an essential part of the RSHE curriculum
- Read and follow this policy in conjunction with the school's main safeguarding policy, KCSIE, Acceptable Use Policy and Code of Conduct
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)

- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the [20 Safeguarding Principles for Remote Lessons](#) infographic which applies to all online learning
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as *copyright and GDPR*
- Be aware of security best-practice at all times, including password hygiene (*'you would never share your toothbrush...'*) and phishing strategies.
- Prepare and check all online source and resources before using
- Encourage pupils/students to follow their acceptable use policy at home as well as at school, remind them about it and enforce school sanctions
- Take a zero-tolerance approach to bullying (including low-level sexual harassment)
- Receive regular updates from the Online Safety Champion and have a healthy curiosity for online safeguarding issues
- Model safe, responsible and professional behaviours in their own use of technology. This includes outside the school hours and site, and on social media, in all aspects upholding the reputation of the school and of the professional reputation of all staff.

2.5 Network Manager & Technical Support

Key responsibilities:

- Support the HT and DSL team as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards
- Work closely with the designated safeguarding lead / online safety champion / data protection officer to ensure that school systems and networks reflect school policy
- 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
- 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
- Monitor the use of school technology and that any misuse/attempted misuse is identified and reported in line to the Headteacher
- Work closely with the Headteacher and School Business Manager to ensure that they understand who the nominated contacts are and what they can do / what data access they have. Advise on the implications of all existing services and changes to settings that the school might request – e.g. for YouTube restricted mode, internet filtering settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Google G Suite.

2.6 Volunteers and contractors (including tutors)

Key responsibilities:

- Read, understand and adhere to the acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety champion
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications

- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session**, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

2.7 Pupils

Key responsibilities:

- Read, understand and adhere to the pupil acceptable use policy (AUP)
- Treat **home learning during any isolation/quarantine or bubble/school lockdown** in the same way as regular learning in school and behave as if a teacher or parent were watching the screen
- Avoid any private communication or use of personal logins/systems to communicate with or arrange meetings with school staff or tutors
- Understand the importance of reporting abuse, misuse or access to inappropriate materials, including any concerns about a member of school staff or supply teacher or online tutor
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else (**The Priory School Keep Safe code - tell a trusted adult**).
- 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

2.8 Parents/Carers

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it
- Upon entry to the school, parents will also sign their consent relating to the **use of the school's internet** and the **school's use of their child's digital image** e.g. on social media – this can be updated by the parent at any time.
- Consult with the school if they have any concerns about their children's and others' use of technology
- Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to avoid video calls in a bedroom if possible and if not, to ensure the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc. and the background blurred or changes where possible.
- If organising private online tuition, remain in the room if possible, ensure the child knows tutors should not arrange new sessions directly with the child or attempt to communicate privately.

2.9 FPS Facebook Groups

Key responsibilities:

- 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

3. Education and Training

3.1 Curriculum

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 subject leaders, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

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

3.2 Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach.

- A planned online safety curriculum should be provided as part of Computing / PHSE – particularly around the safe use of Google Education Suite.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities e.g. Safer Internet Day.
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues.
- Pupils should be helped to understand the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.

3.3 Parents/Carers

Parents play an essential role in the education of their children and in the monitoring / regulation of children's online behaviours. However, keeping up-to-date with the ever-changing online safety risks and issues is a real challenge.

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 Priory School will therefore seek to provide information and awareness to parents through:

- Half-termly Curriculum Newsletters
- Parent information evenings (including dedicated Dorset Safer Schools Community Team events)
- Newsletters

- A dedicated Online Safety webpage via the school website with links to CEOP <https://www.ceop.police.uk/Safety-Centre/> and childnet <https://www.childnet.com/parents-and-carers>

4. Data protection and data security

GDPR information is in our Data Protection Policy.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the Headteacher, School Business Manager and Governors will seek to apply.

All pupils, staff, governors, volunteers and parents are bound by the school's data protection policy and agreements. Rigorous controls on the school network, firewalls and filtering all support data protection.

The headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first.

5. 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."*

The school's information management systems are secured by TurnITon using Ruckus unleashed wireless security and their in-house network 'Discover'. Virus protection is installed and updated regularly. The school uses broadband with appropriate firewall and filters as recommended by provider **South West Grid for Learning**.

There are three types of appropriate monitoring. 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 The Priory School, we use physical monitoring alongside our web filtering system to control internet and web access in school. When pupils log into any school system on a personal device, activity may also be monitored here.

Where children are using their own devices at home, parents agree to supervise and ensure that potential parental controls are in place **(see appendix 4 loaned laptop indemnity agreement)**.

Advice for parents can be found at <https://www.internetmatters.org/parental-controls/>

6. Electronic communications

6.1 Email

- Pupils at this school use Gmail & the messaging function within Google Classroom

- Staff at this school use Office 365 or Gmail. Staff are required to use the office@prioryceprimary.co.uk account when responding directly with parents

This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use (including the message function in Google Classroom, our virtual Learning Environment) are as follows:

- Use of a different platform 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) or to the Headteacher (if by a staff member).
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Appropriate behaviour is expected at all times, and systems should not be used to send inappropriate materials or language which is or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which (for staff) might bring the school into disrepute or compromise the professionalism of staff. **Pupils should report any offensive email or chat to the class teacher.**
- Pupils and staff are allowed to use the email system for reasonable (not excessive, not during lessons) personal use but should be aware that all use is monitored, their emails may be read and the same rules of appropriate behaviour apply at all times. Emails using inappropriate language, images, malware or to adult sites may be blocked and not arrive at their intended destination.
- The forwarding of chain letters is not permitted.

6.2 Video Conferencing

The school uses Zoom and Google Meet as its primary virtual conferencing platforms. We have developed a code of conduct for pupils and staff:

Teachers

- Never join a meeting with a single child (groups of 2 or above minimum) unless you are in an open space in school
- Wear professional attire
- Use a background to block images of your home and where you live
- Mute all, except for registration
- Ensure all users have left the meeting before leaving yourself
- Ensure all recording disabled
- Only admit named pupil accounts

Children

- Be appropriately clothed for school (NOT pyjamas)
- Younger children must be in a shared space with an adult to hand e.g. kitchen table. Older children must have their door open and an adult within earshot - Parents must not be 'seen on screen' as this is a time for the children to see one another .
- Calling out, rude gestures, inappropriate use of the chat bar etc. will not be tolerated – access to Google Meet will be removed.
- Pupils must not set up their own Google Meet events and you must never join a meeting without the adult host present (*this should have been disabled*).
- To ask a question, please use the 'Raise your hand' button.
- Be kind and respectful.

7. 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. SLT have responsibility for updating the content of the website. The site is hosted by Wordpress.

The DfE has determined information which must be available on a school website. [Maintained Schools: website audit](#)

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

- School have the same duty as any person or organisation to respect and uphold copyright law. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published unless direct consent has been given.

8. Cloud platforms

At The Priory School, we use Google for Education's G Suite as our main virtual learning platform. In Year R, Tapestry is also used. We use CPOMs to store safeguarding information. Our main MIS (Management Information System) is SIMs. Our main communication and payment platform is SCOPAY. The school will explore other online platforms to facilitate online learning and parent meetings as appropriate e.g. schoolcloud / IXL /

Privacy notices relating to Google Education is available [here](#):

The following principles apply:

- The Headteacher, Network Manager and School Business Manager have two-factor authentication and the authority to amend settings and add new users.
- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such.
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen.
- Pupil images/videos are only made public with parental permission.
- Only school-approved platforms are used by pupils or staff to store pupil work (Google Classroom / Google Drive / Tapestry).

9. 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. This consent is part of the **Pupil Induction Information Pack**.

Whenever a photo or video is taken/made, the member of staff taking it will check the latest database before using it for any purpose. **An up to date consent list is available on G Drive for all staff to access.**

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), unless specific consent has been given.

All staff are governed by their contract of employment and the school's Acceptable Use Policy, which covers the use of mobile phones/personal equipment for taking pictures of pupils, and where these are stored.

At The Priory School **SLT members of staff only** may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (*NB – many phones automatically back up photos*).

Photos are stored on the Priory Education G Drive account in line with the retention schedule of the school Data Protection Policy.

Staff and parents are reminded regularly (and certainly at large school events) 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.

Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children

Pupils are advised to be very careful about placing any personal photos on social media and YouTube accounts. 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.

10. Social media

10.1 The Priory School's Social Media Presence – Twitter and YouTube

Even though we do not have a Facebook account, 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.

SLT are responsible for managing our Twitter account, which is primarily viewed as our 'Highlights Reel' to promote the good work of the school (@PrioryCEPrimary).

The Headteacher manages the school's YouTube platform, using the Headteacher's school Google account: head@prioryceprimary.co.uk. This platform is primarily used to share school events with our community, especially during periods of lockdown.

10.2 Staff, pupils' and parents' Social Media presence

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or FPS groups.

If parents 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 should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+), but the school occasionally has to deal with issues arising on social media with pupils well under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use.

However, 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 cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.

Parents can best support this by talking to their children about the apps, sites and games they use (you don't need to know them – ask your child to explain it to you), with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).

Please refer to the [Top Tips for Parents](#) poster and the [Children's Commission Digital 5 A Day](#).

Email is the official electronic communication channel between parents and the school, and between staff and pupils (NB Google Classroom 'chat' may also be used by pupils during a period of lockdown or quarantine).

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 or governor 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 children accounts.

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

*** Any attempt to do so may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).*

Staff are reminded that they are obliged not to bring the school or profession into disrepute and the easiest way to avoid this is to have the strictest privacy settings and avoid inappropriate sharing and oversharing online. 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 or local authority.

All members of the school community are reminded that, particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see above) and permission is sought before uploading photographs, videos or any other information about other people.

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

11. Device usage (including mobile phones in school)

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

11.1.1 Pupils

- **Pupils are not allowed to use personal mobile phones in school.** Any attempt to use a phone in lessons without permission or to take illicit photographs or videos will lead to the temporary withdrawal of mobile privileges (*minimum 4 weeks depending on the circumstances*).
- Important messages and phone calls to or from parents can be made at the school office, which will also pass on messages from parents to pupils in emergencies.
- **Pupils in Year 5 and 6** are allowed to bring mobile phones to school but they must be turned off and handed in to the class teacher on arrival.
- **The school does not take any responsibility for any damage to pupil phones** that may occur during the time they are in school.
- The school has the right to take, examine and search any device that is suspected of unauthorised use at any time.

11.1.2 Staff, Visitors, Governors and Contractors

- Mobile phones should be **switched to silent (*)** when entering the school **and should never be used for personal purposes in front of pupils.**

**The caretaker only is able to receive school-related calls on his mobile phone.*

- If teachers, visitors, governors or volunteers wish to make or take an emergency call they may use the school main telephone or their own mobile phone in the staff room / one of the designated offices.
- Mobiles phones should not be used (*) (**) to surf the internet, play games or take photographs or recordings of children, staff or other visitors.

** SLT members of staff only may occasionally use personal/school phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy and not in a one-to-one situation, and always moved to school storage as soon as possible.*

*** The School Business Manager and SLT only may occasionally use personal/school phones to contact supply agency cover via WHATSAPP messaging or equivalent.*

- The Bluetooth function of the mobile phone must not be used to send images or files to other phones.
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to pupils, staff or visitors to the school.

- It is unacceptable to take a picture or video of a member of staff without their consent.
- The school accepts no responsibility for replacing lost, stolen or damaged mobile phones.
- Teachers, supply teachers, volunteers and visitors must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence.
- Staff should only use school approved encrypted removable hard drives in school. Confidential or personal data relating to staff or pupils must *never* be stored on a staff's personal memory stick or hard drive.

11.1.3 Parents

- **Parents** should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

Teachers, supply teachers, volunteers or visitors who infringe the rules set out in this document could face being banned from the school grounds.

11.2 Network / internet access on school devices

	School Devices		Personal Devices		
	School owned (or authorised) for single user e.g. SEND laptop	School owned for multiple users	Pupil owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Only 5 & 6 & handed in on entry	Yes	Yes
Full/Partial network access depending on user access	Yes	Yes	No	No	No
Internet only			No	Yes	Yes

- **Pupils** are not allowed networked file access via personal devices. However, they are allowed to access the school wireless internet network for school-related internet use within the framework of the acceptable use policy (DfE provided laptops for vulnerable pupils). All such use is monitored.
- **Home devices** for vulnerable pupils from the DfE scheme may be issued to some pupils. If devices are to be taken home, it is the parents responsibility to add sufficient parental controls to ensure that children can only access required applications (see **laptop indemnity letter appendix 4**).

- **All Staff & Governors** can access the relevant G Drives on private devices, however use must comply with this policy.
- **Volunteers & Contractors** can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy.
- **Parents** (unless acting in their capacity as staff members or Governors) have no access to the school network or wireless internet on personal devices.

11.3 Devices used for 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/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher.

Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

12. 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.

13. Handling online-safety concerns and incidents

General concerns must be handled in the same way as any other **safeguarding** or **behaviour** concerns; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should share any concerns, however small, to the online-safety champion/ DSL to contribute to the overall picture.

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). The school cannot accept liability for the material accessed, or any consequences of Internet access.

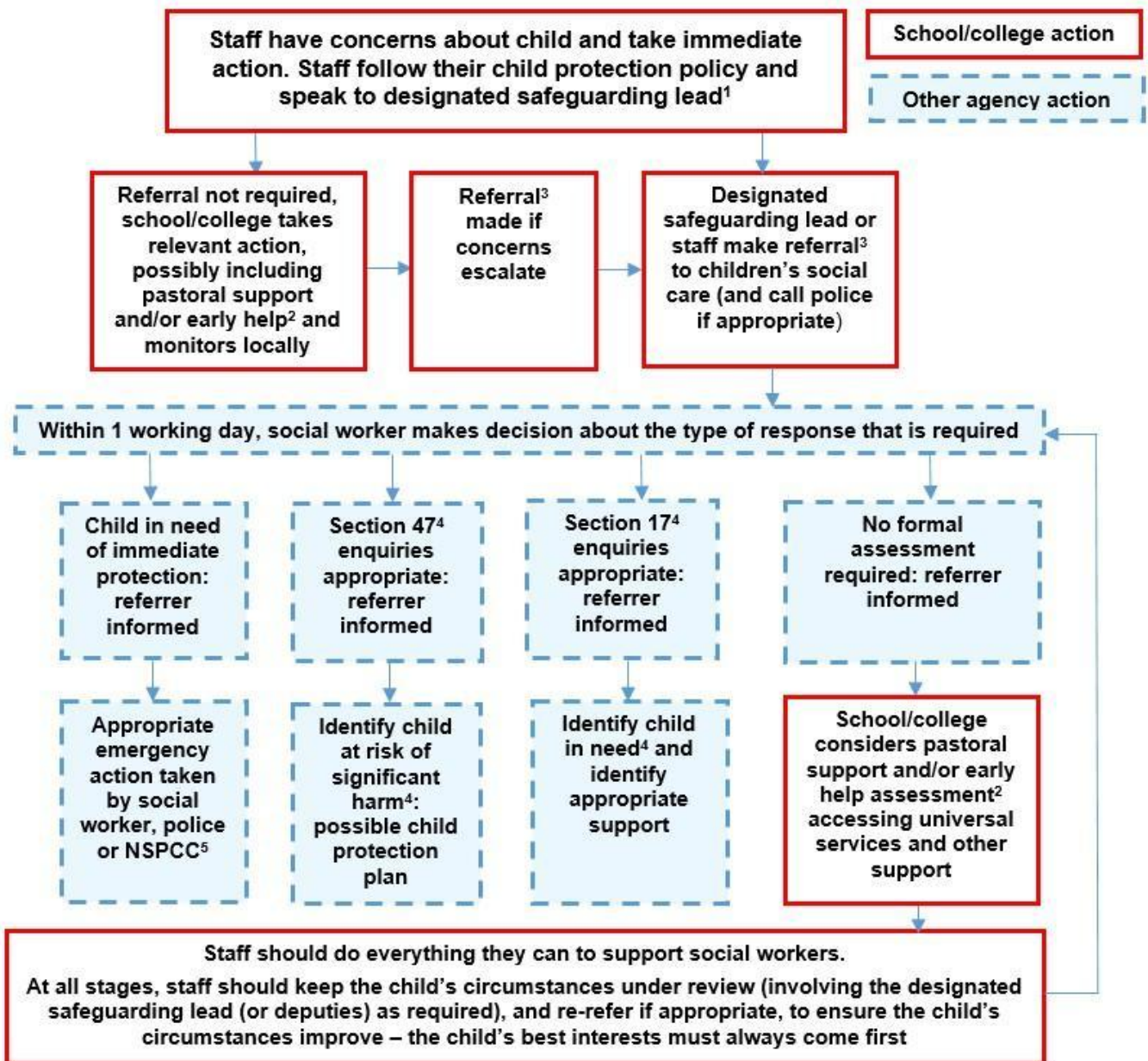
All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

- **Any suspected online risk or concern** should be reported to the online safety champion / DSL on the same day – where clearly urgent, it will be made by the end of the lesson. **Appendix 2 (Online Safety Reporting Log)** will need to be completed by the Online Safety Champion or DSL). If the school needs to review a website or device, then **Appendix 1 (Online Safety Recording Form)** will need to be completed for evidence. In all cases a **CPOMS** entry will be added in line with the school's Child Protection Policy.
- **Any concern/allegation about staff misuse** is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complainant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

- The school will actively seek support from other agencies as needed (i.e. the local authority, SSCT, UK Safer Internet Centre’s Professionals’ Online Safety Helpline, NCA CEOP, BCP First Response Team).
- **We will always 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 and upskirting; see section below).

13.1 Actions where there are concerns about a child

We will follow the following flowchart where online safety concerns lead to a concern about a child:



13.2 Sexting

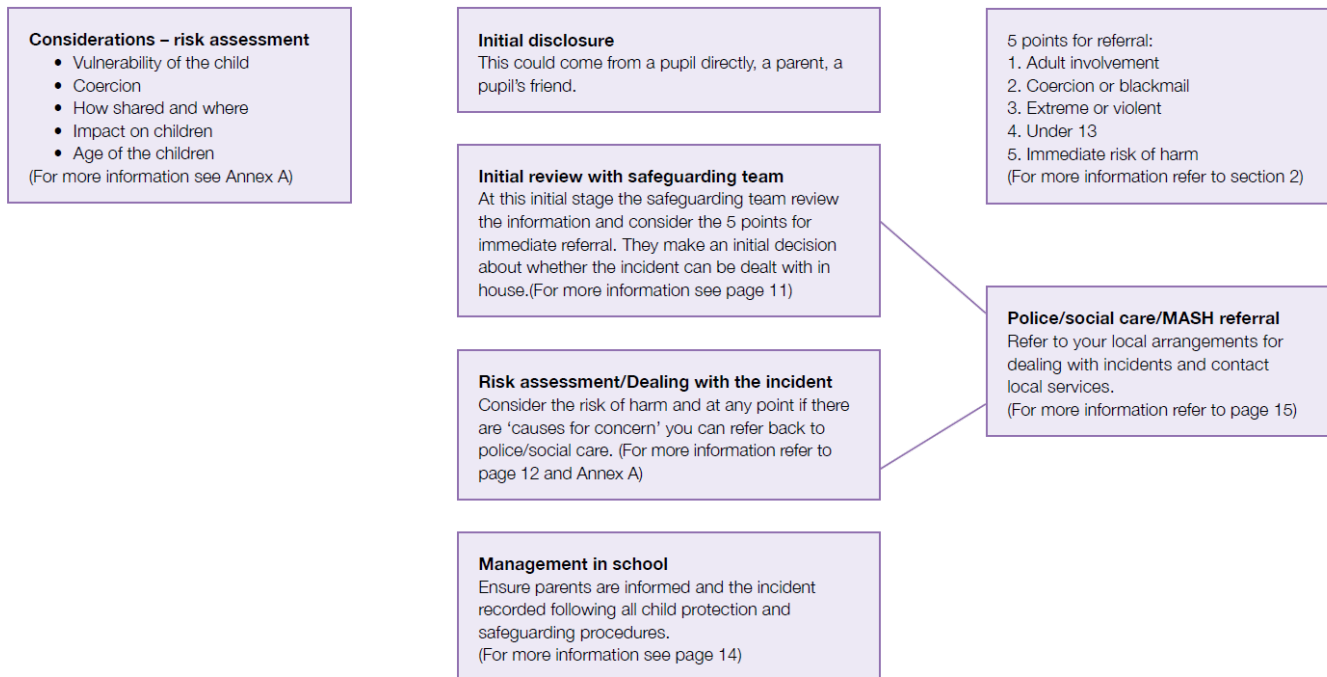
All schools (regardless of phase) should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (also referred to as ‘youth produced sexual imagery’) in schools. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

There is a one-page overview called [Sexting; how to respond to an incident](#) for all staff to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety champion to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, [Sexting in Schools and Colleges](#) to decide next steps and whether other agencies need to be involved.

It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The following flowchart is a useful summary of the actions to be taken.



13.3 Upskirting

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

13.4 Online Bullying (sometimes referred to as Cyberbullying)

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from ‘Group Chat banter’ and arguments between peers when playing online games.

Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

13.5 Sexual violence and harassment

DfE guidance on sexual violence and harassment is referenced in Keeping Children Safe in Education and also a document in its own right. 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.

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

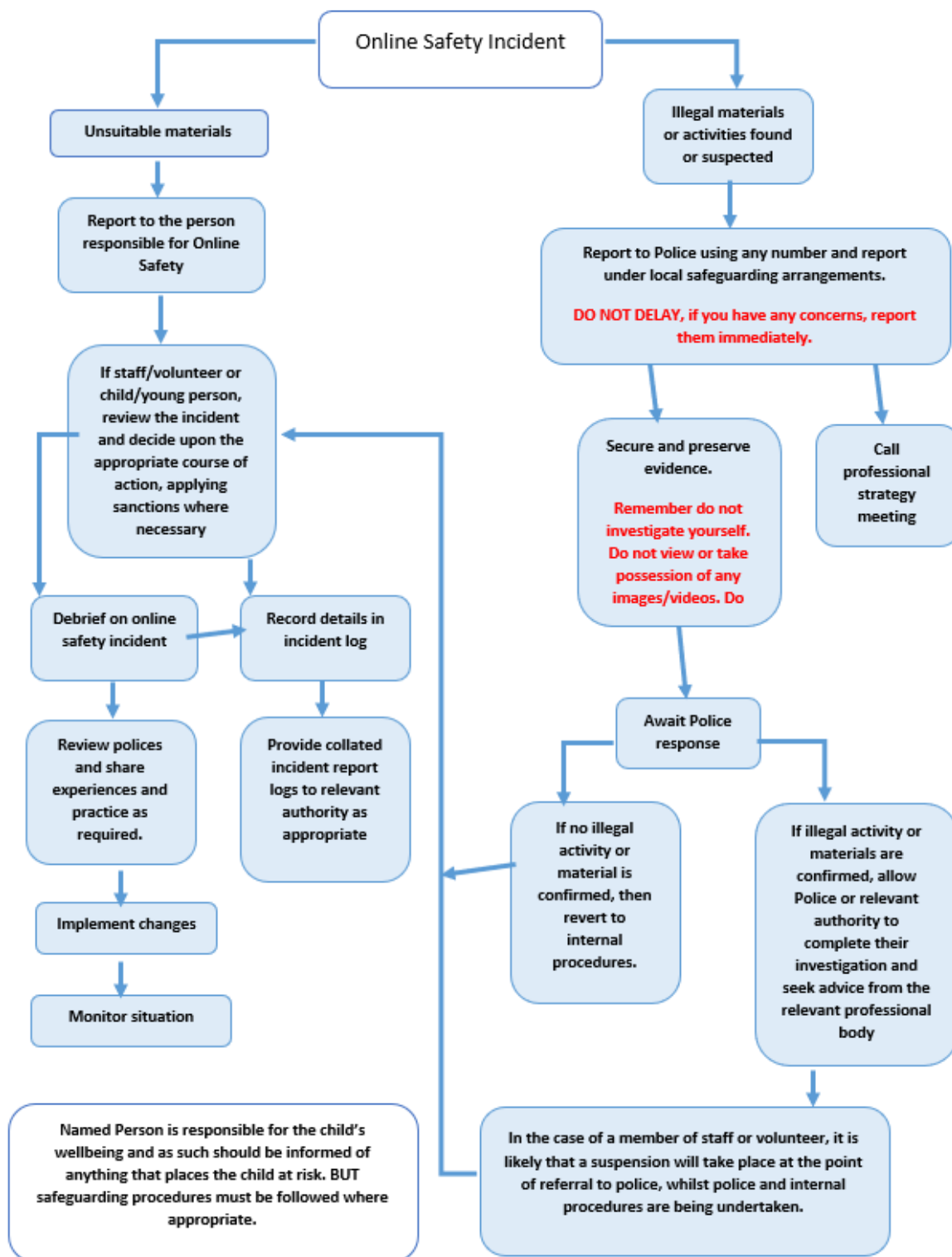
Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). These are defined in the relevant Acceptable Use Policy as 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.

It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that the same applies for any **home learning** that may take place in future periods of closure/quarantine etc. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology.

13.7 Illegal Incidents Flowchart and Procedure

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 flowchart and procedure below (**completing Appendix 1 and 2**).



- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).

· Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the reporting form (except in the case of images of child sexual abuse – see below)

· Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

· If the content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

· Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes.

13.8 Social media incidents

See the social media section in this document for rules and expectations of behaviour for children and adults in the The Priory 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, The Priory 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.

13.9 Prevent

In accordance with the Prevent Strategy, which aims to prevent children and young people being exposed to extremist views and at risk of radicalisation, staff are all trained in protecting children from extremist material online. Through this training, staff are aware of how the internet is used to radicalise people.

Filtering should prevent access to such extremist sites but any material accessed at school should be treated as an online safety incident and dealt with accordingly. Disclosures or concerns regarding exposure outside of school should be treated as a safeguarding incident and dealt with in accordance with the Safeguarding policy and procedures (cf. Safeguarding policy).

Parents and carers are informed about the risks of radicalisation and extremism via newsletters and a dedicated page on the school website.

13.10 Indecent Images and pornography

There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This would lead to a criminal investigation and the individual being barred from working with children, if proven.

Staff should not use equipment belonging to the school to access any pornography; neither should personal equipment containing such material be brought into the workplace. This would raise serious concerns about the suitability of the adult to continue working with children.

14. Monitoring and evaluation

This occurs through the process of the curriculum monitoring, evaluation and review programme and is reported to the Governing Body by the Online Safety Champion. Online Safety practice and perceptions are reviewed through parent, pupils and staff questionnaires, pupil interviews and work sampling.

15. Policy Version History

Date	Comments / Reviewed:
Sep 2017	E-Safety Policy written by Simon Croutear, acting Headteacher
Sep 2019	New online safety policy written by Simon Croutear, Online Safety Champion <ul style="list-style-type: none"> - Amended sections on use of mobile phone - Link to new online safety curriculum programme of study - New network manager support by TurnITOn & SWGfl broadband provider
Apr 2021	Fully revised online safety policy written by Paul Ruffle, new Online Safety Champion based on template policies by SWGfl and LGfl and 360Safe following lessons learnt during coronavirus crisis. <ul style="list-style-type: none"> - New roles and responsibilities guidance - New remote learning safety procedures (including video conferencing & cloud platforms e.g. Google Drive / Classroom & loaned devices) - New section on social media code of conduct - Amended sections on use of digital images and video - New section on handling online safety concerns and misuse incl. sexting and upskirting - Updated section on use of personal devices - Link to new AUP
July 2022	Minor changes relating to role titles and responsibilities
July 23	Discussed policy as part of 360 safe audit at handover with new SLT. Still reflects current practice, but does not include 4C's. Decision that future full review needed to reflect the changes of KCSIE (Sept 23) and updated SWGFL template policy (Oct 2023)



Online Safety Policy

Appendix 1 – Recording Form for investigating devices / internet sites

Group: _____
Date: _____
Reason for investigation: _____

Details of first reviewing person

Name: _____
Position: _____
Signature: _____

Details of second reviewing person

Name: _____
Position: _____
Signature: _____

Name and location of computer used for review (for web sites):

<i>Web site(s) address / device</i>	<i>Reason for concern</i>

Conclusion and Action proposed or taken



Appendix 3 – Legislation

School staff should be aware of the legislative framework which currently surrounds the use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Computer misuse act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data protection act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject’s rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of information act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious communications act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of investigatory powers act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
 - Ascertain whether the communication is business or personal;
 - Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, designs and patents act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for noncommercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal justice & public order act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

-

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour;

or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and religious hatred act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from harassment act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of children act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Sexual offences act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) and you arrange to meet them or travel to meet them (anywhere in the world) with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public order act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the **Racial and Religious Hatred Act 2006** it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene publications act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human rights act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data.

(see template policy in these appendices and for DfE guidance -

<http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation>)

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent/carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:

<https://www.gov.uk/guidance/what-maintained-schools-must-publish-online>


Serious Crime Act 2015

Introduced new offence of sexual communication with a child. Also created new offences and orders around gang crime (including CSE)

Criminal Justice and Courts Act 2015

Revenge porn – as it is now commonly known – involves the distribution of private and personal explicit images or video footage of an individual without their consent, with the intention of causing them embarrassment and distress. Often revenge porn is used maliciously to shame ex-partners. Revenge porn was made a specific offence in the Criminal Justice and Courts Act 2015. The Act specifies that if you are accused of revenge porn and found guilty of the criminal offence, you could be prosecuted and face a sentence of up to two years in prison.

For further guidance or support please contact the [Revenge Porn Helpline](#)





The Priory CE VA Primary School

Online Safety Policy

Appendix 4 – Loaned Laptop Indemnity

Wick Lane
Christchurch
Dorset
BH23 1HX

Telephone (01202) 484105

Fax (01202) 488702

Email: office@prioryceprimary.co.uk

Website: <https://prioryschool.dorset.sch.uk>

Date

Dear Name of Parent/Carer,

We have provided name of child with a loan device (e.g. Chromebook) for reason (e.g. home learning).

Headteacher: Mr P Ruffle
The 'Keeping Children Safe in Education' obliges schools and colleges in England to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system". Please be aware that you will not have this filtering system in place at home therefore, please ensure you are monitoring the content that name of child is accessing at all times.

We would be grateful if you would please sign and return the reply slip below to confirm safe receipt of this device. You are also signing to agree this will be looked after and returned by you as the parent/carer to the School Office in a clean and good working order.

Please advise the School Office of any issues with the device as soon as possible during the loan period.

The device (Make, model no. & serial no.) must be returned when school resumes as normal following lockdown or when requested.

With kind regards,

The Priory School Office

Remote Learning - Loan of Device Reply Slip

I confirm I have received a name of device (Make, model no. & serial no. 5CD8366J4Y) on loan from the Priory School for the following pupil(s):

Signed: _____

Date: _____

Name: _____