Ecclesfield and Coit Primary School

Online Safety Policy

	Ecclesfield	Coit
Designated Safeguarding Lead (DSL) team	Phullippa Robinson	Charlotte Zadrozny
Online-safety lead (Must be Safeguarding Trained)	Hannah Travers	Helen Fenlon
Online-safety / safeguarding link governor	Kevin Corke	Kevin Corke
PSHE/RSHE lead	Sheryl Garner	Helen Fenlon
Network manager / other technical support	Blue Box IT	Blue Box IT
Date this policy was reviewed and by whom	September 2025	September 2025
Date of next review and by whom	September 2026	September 2026

What is this policy?

This Online Safety Policy outlines the commitment of Ecclesfield and Coit Primary Schools to safeguard members of our school community online in accordance with statutory guidance and best practice. This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Ecclesfield and Coit Primary School believe in and implement a rigorous system in relation to the risks of being online. As well as encouraging children, irrespective of race, disability, sexual orientation or religious beliefs, to access the online world and use it to enhance their thinking and learning, we also promote the need to keep children safe especially those we deem as vulnerable. Children now live in a world full of online communication and technologies and at Ecclesfield and Coit Primary School we want to promote the benefits of this and how it can support learning and our own personal interests. However, we want to educate children so that they know: How to keep themselves safe online; who to talk to if they feel at risk, what potential risks there are in the online world and what to do if they ever receive threatening/abusive messages or emails.

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' (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 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 Safeguarding Policies. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

This policy along with the AUP (Acceptable Use Policy, see Appendix) is applicable to all stakeholders so that a whole school approach is achieved and so that online Safety is embedded at Ecclesfield and Coit Primary. It also applies to the use of personal digital technology on the school site (where allowed).

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.

This policy applies to all members of the school (including staff, Board of Governors, students / pupils, volunteers, mothers / fathers / carers, work placement students, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

- **The Education and Inspections Act 2006** empowers Executive 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. This applies to incidents of cyber-bullying, or other Online Safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

- **The Education Act 2011** gives the school the power to confiscate and search the contents of any mobile device if the Executive Headteacher believes it contains any illegal content or material that could be used to bully or harass others. https://www.gov.uk/government/publications/searching-screening-and-confiscation

- The school will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform mothers / fathers / carers of incidents of inappropriate Online Safeguarding behaviour that takes place out of school / college. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe In Education** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools and colleges **should** do and sets out the legal duties with which schools and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children**

- **Counter-Terrorism and Security Act 2015** From 1 July 2015 all schools, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.

  The statutory guidance on the Prevent duty summarises the requirements on schools and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.

  https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

This Online Safety Policy was approved by the *school governing body on:*	September 2023
The implementation of this Online Safety Policy will be monitored by:	Hannah Travers/Helen Fenlon Safeguarding Team Senior Leaders
Monitoring will take place at regular intervals:	Weekly Smoothwall monitoring Regular online safety teaching and learning monitoring
The *governing body* will receive a report on the implementation of the Online Safety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Termly within Governors Meetings
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	September 2026
Should serious online safety incidents take place, the following external persons/agencies should be informed:	LADO DPO

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- *logs of reported incidents*
- *Filtering and monitoring logs*
- *internal monitoring data for network activity*

- *surveys/questionnaires of: learners, parents and carers, Staff*
- *Pupil Interviews and discussion groups*

How will this policy be communicated?

This policy can only impact upon practice if it is a (regularly updated) living document. It must be accessible to and understood by all stakeholders. It will be communicated in the following ways:

- Available on the internal staff network/drive
- Shared with staff annually
- Part of school induction pack for all new staff (including temporary, supply and non-classroom-based staff)
- Integral to safeguarding updates and training for all staff (especially in September refreshers)
- Clearly reflected in the Acceptable Use Policies (AUPs) for staff, volunteers, contractors, governors, pupils and parents/carers (which must be in accessible language appropriate to these groups).
- AUPs issued to whole school community, on entry to the school, with annual reminders of where to find them if unchanged, and reissued if updated after annual review
- Class AUPs are displayed around school/corridors (not just in computing corridors/classrooms)
- 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 Ecclesfield and Coit Primary School's 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, respectful and positive 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 Ecclesfield and Coit Primary School(including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, governors, volunteers, contractors, students/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.

Executive Headteacher– Louise Chadwick

Key responsibilities:

- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- 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 Sheffield Safeguarding Children Partnership.
- 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
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- 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
- The headteacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- 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 – [Phillippa Robinson/Charlotte Zadrozny, Hannah Travers / Helen Fenlon]

Keeping Children Safe in Education states that:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."

They (the DSL) "are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college"

*They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety lead, but not the overall responsibility. In Sheffield the Online Safety Lead must be trained to DSD standards.

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety]. This **lead** responsibility should not be delegated"
- Where the online-safety curriculum lead is not the named 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.
- Where the school has an Online Safety Curriculum Coordinator who is not a fully trained part of the safeguarding team ensure that roles are clearly defined so that safeguarding and the DSL's overarching responsibility for it is not compromised.
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs, or the named person with oversight for SEN in a college and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies."

- Take day-to-day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Remind staff of safeguarding considerations as part of a review of remote learning procedures and technology, including that the same principles of online safety and behaviour apply
- 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 safeguarding and "undertake Prevent awareness training.
- Monitor the use of school technology, online platforms and social media presence and that any misuse/attempted misuse is identified and reported in line with school policy
- 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.
- 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. Examples can be seen in the Sheffield RSHE Curriculum
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents.
- Communicate regularly with SLT and the designated safeguarding and online safety governor/committee to discuss current issues (anonymised), review incident logs and filtering/change control logs 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.
- Ensure adequate provision for staff to flag issues when not in school and for pupils to disclose issues when off site, especially when in isolation/quarantine/lockdown, e.g. a safe, simple, online form on the school home page about 'something that worrying me' that gets mailed securely to the DSL inbox/
- Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are also aware (Ofsted inspectors have asked classroom teachers about this).
- Be aware and make judicious use of safeguarding reports that are produced by the schools Internet Monitoring Service by working in conjunction with technical teams.
- Make key decisions on allowing access to sites and apps in schools by relaxing either temporarily or permanently some of the filtering setting within the schools filtering and monitoring system and ensure that these decisions are logged. The DSL should prioritise keeping children safe but "be careful that 'over blocking' does not lead to unreasonable restrictions" (KCSIE)

- Receive relevant and regularly updated training and facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children
    - cascade knowledge of risks and opportunities throughout the organisation
- Pay particular attention to **online tutors**, both those engaged by the school as part of the DfE scheme who can be asked to sign the contractor AUP, and those hired by parents share the Online Tutors – Keeping Children Safe poster at parentsafe.lgfl.net to remind parents of key safeguarding principles
- Work with the Headteacher to ensure the school website meets statutory DfE requirements

Governing Body, led by Online Safety / Safeguarding Link Governor Kevin Corke

The DfE guidance "Keeping Children Safe in Education" states:
"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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
- 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
- "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…"
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)

- 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 lead / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety curriculum coordinator is not the named DSL or deputy DSL, ensure that there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Work with the DPO, DSL and headteacher to ensure a 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 B; check that Annex D on Online Safety reflects practice in your school
- Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction.
- Ensure appropriate filters and appropriate monitoring systems are in place [but…] be careful that 'overblocking' 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 – you may wish to refer to 'Teaching Online Safety in Schools 2019' and investigate/adopt the UKCIS cross-curricular framework 'Education for a Connected World – 2020 edition' to support a whole-school approach

Curriculum Leads

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme (Sheffield RHE scheme)

This will be provided through:

- a discrete programme
- PHSE and SRE programmes
- A mapped cross-curricular programme
- assemblies and pastoral programmes
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

All staff

Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e. policies and protocols are in place for the use of online communication

technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

Key responsibilities:

- Recognise that **RSHE** is now statutory and that it is a whole-school subject requiring the support of all staff; online safety has become core to this new subject
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up
- Have an awareness of current online safety matters/trends and of the current school Online Safety Policy and Practices.
- Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are and immediately report any suspected misuse or problem for investigation/action.
- Read Part 1 of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, it is good practice for all staff to read the whole document).
- Read and follow this policy in conjunction with the school's main safeguarding policy
- Record online-safety incidents in the same way as any safeguarding incident and report in accordance with school procedures.
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Sign and follow the staff acceptable use policy and code of conduct/handbook
- Notify the DSL/OSL if policy does not reflect practice in your school and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all school activities as part of a whole school approach in line with the RSHE curriculum, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)
- Whenever overseeing the use of technology in school or for homework or remote teaching, encourage and talk about appropriate behaviour and how to get help and consider potential risks and the age-appropriateness of websites (find out what appropriate filtering and monitoring systems are in place)
- 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 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.

- Notify the DSL/OSL of new trends and issues before they become a problem

- Take a zero-tolerance approach to bullying and sexual harassment
- Read UKCIS Sharing Nudes and Semi –Nudes: How to Respond to an Incident.
- 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 safeguarding issues
- All digital communications with learners and parents/carers are on a professional level and only carried out using official school systems
- 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 and here

PSHE / RSHE Lead/s – Sheryl Garner and Helen Fenlon

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 / RSHE.
- Work closely with the Computing subject leader to avoid overlap but ensure a complementary whole-school approach, and with all other lead staff to embed the same whole-school approach

Computing Lead - Cathy Hill and Amber Machin

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 RSHE lead to avoid overlap but ensure a complementary whole-school approach
- Work closely with the DSL/OSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Subject / aspect leaders

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Look for opportunities to embed online safety in your subject or aspect, especially as part of the new RSHE curriculum, and model positive attitudes and approaches to staff and pupils alike
- Consider how the UKCIS framework Education for a Connected World and Teaching Online Safety in Schools can be applied in your context
- Work closely with the DSL/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

Network Manager/technician – BlueBox IT (Alongside Online Safety Co-ordinator)

The DfE Filtering and Monitoring Standards says:

"Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider."

"Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet

the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support."

"The IT service provider should have technical responsibility for:

- *maintaining filtering and monitoring systems*
- *providing filtering and monitoring reports*
- *completing actions following concerns or checks to systems"*

"The IT service provider should work with the senior leadership team and DSL to:

- *procure systems*
- *identify risk*
- *carry out reviews*
- *carry out checks"*

"We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible, and it must be possible to make prompt changes to your provision."

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the** procedures, rules and safeguards
- Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- Meet the RSHE lead to see how the online-safety curriculum delivered through this new subject can complement the school IT system and vice versa, and ensure no conflicts between educational messages and practice.
- Work closely with the designated safeguarding lead / online safety lead / data protection officer/nominated contact 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 and ensure safeguarding reports are manageable and appropriately shared,

- 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
- they are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively 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
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to a member of the safeguarding team for investigation and action
- the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person (see appendix 'Technical Security Policy template' for good practice).

Data Protection Officer (DPO) – Dee Whitmore

Key responsibilities:

- NB – this document is not for general data-protection guidance;
- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), especially this quote from the latter document:
- "GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information **must not be allowed** to stand in the way of promoting the welfare and protecting the safety of children."

The same document states that the retention schedule for safeguarding records may be required to be set as 'Very long term need (until pupil is aged 25 or older)'. However, some local authorities require record retention until 25 for <u>all</u> pupil records.

- Work with the DSL, headteacher and governors to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above. You may be interested in the discounts for LGfL schools for three market-leading GDPR compliance solutions at gdpr.lgfl.net
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited
- Ensure that photographs are stored appropriately, shared in line with consent and kept for appropriate timescales.

Schools Monitoring and Filtering Provider – Smoothwall (via Bluebox IT)

Key responsibilities:

- To ensure all services are managed on behalf of the school in line with school policies, following data handling procedures as relevant
- Work closely with the DSL and DPO to ensure they understand who the nominated contacts are and what they can do / what data access they have, as well as the implications of all existing services and changes to settings that you might request – e.g. for YouTube restricted mode, internet filtering and monitoring settings, firewall port changes, pupil email settings, and sharing settings for any cloud services such as Microsoft Office 365 and Google G Suite.
- Ensure the DPO is aware of the GDPR information on the relationship between the school and LGfL at gdpr.lgfl.net

Volunteers and contractors (including tutor)

Key responsibilities:

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator as named in the AUP
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology at school and as part of remote teaching or any online communications
- Note that as per AUP agreement a contractor will never attempt to arrange any meeting, **including tutoring session,** without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.

Pupils

Key responsibilities:

- Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually
- Treat **home learning** 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.
- To understand the importance of adopting safe and responsible behaviours and good online safety practice when using digital technologies outside of school and realise that the school's acceptable use policies cover actions out of school, including on social media
- Remember the rules on the misuse of school technology – devices, mobile devices and logins used at home should be used just like if they were in full view of a teacher.
- 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

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Key responsibilities:

- Read, sign and promote the school's parental acceptable use policy (AUP) provided with new starter material..
- 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, 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.
- Encourage children to engage fully in home-learning and flag any concerns
- 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.

- Further advice available in the Online Tutors – Guidance for Parents and Carers poster at parentsafe.lgfl.net, which is a dedicated parent portal offering updated advice and resources to help parents keep children safe online

How school can support parents and carers

The school will take every opportunity to help parents and carers understand these issues through:

- Parents/carers provided with a Parent AUP (new starter pack)
- publish information about current trends and online issues via the website and newsletters
- seek their permissions concerning digital images etc

Education and curriculum

While regulation and technical solutions are particularly important, their use must be balanced by educating learners to take a responsible approach. The education of learners in online safety is therefore an essential part of the school's online safety provision. Learners need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as
required in all relevant policies and considering online safety whilst planning the curriculum …"

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

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

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

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).

Ecclesfield and Coit will ensure:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning and current trends
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PSHE; RHE English etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

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 / schemes of work (including for SEND pupils) are used as an opportunity to follow this framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Handling online-safety concerns and incidents

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of learners. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

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/RSHE and Citizenship).

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.

Staff should report online safety concerns/issues/incidents as they would any safeguarding concerns/issues, incidents; Staff will ensure these are reported immediately to DSL/DSD in line with our child protection Policy.

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Behaviour Policy (including school sanctions)

- Acceptable Use Policies
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

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 pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made immediately. These should be recorded using CPOMs following verbal discussion with a member of the safeguarding team.

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.

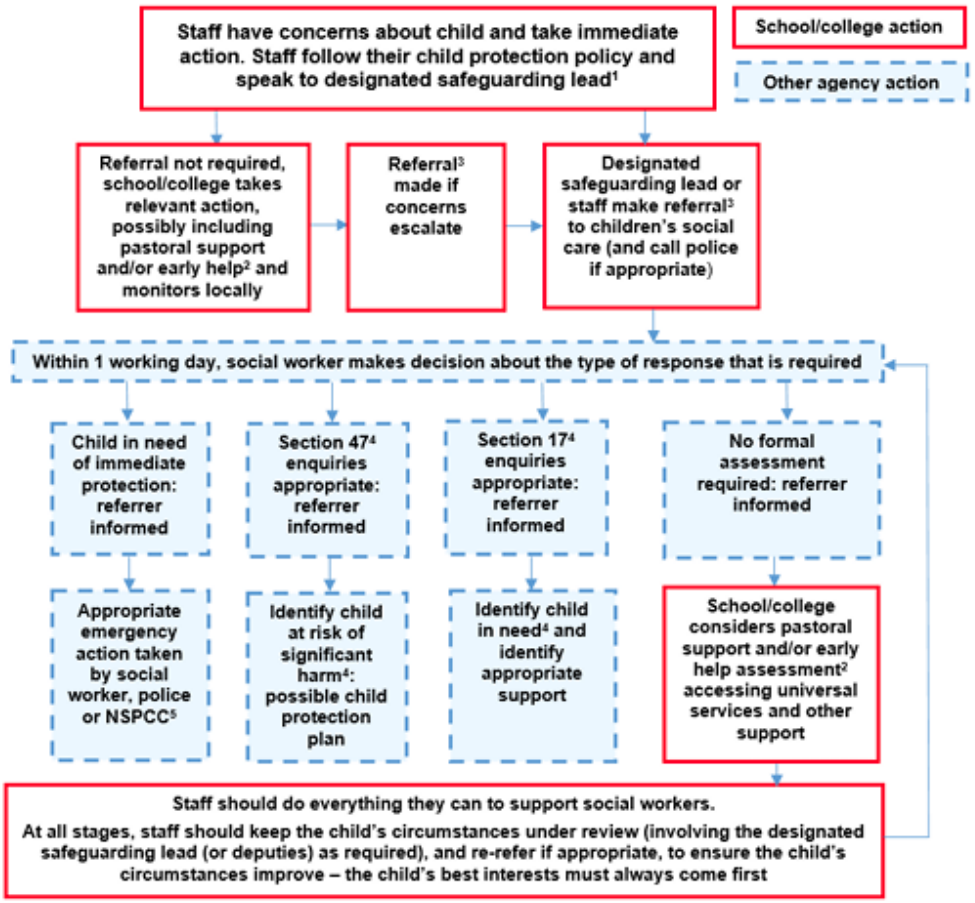
The school will actively seek support from other agencies as needed (i.e. the local authority, SCSP, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and 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 and upskirting; see section below).

The school should evaluate whether reporting procedures are adequate for any future closures/lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

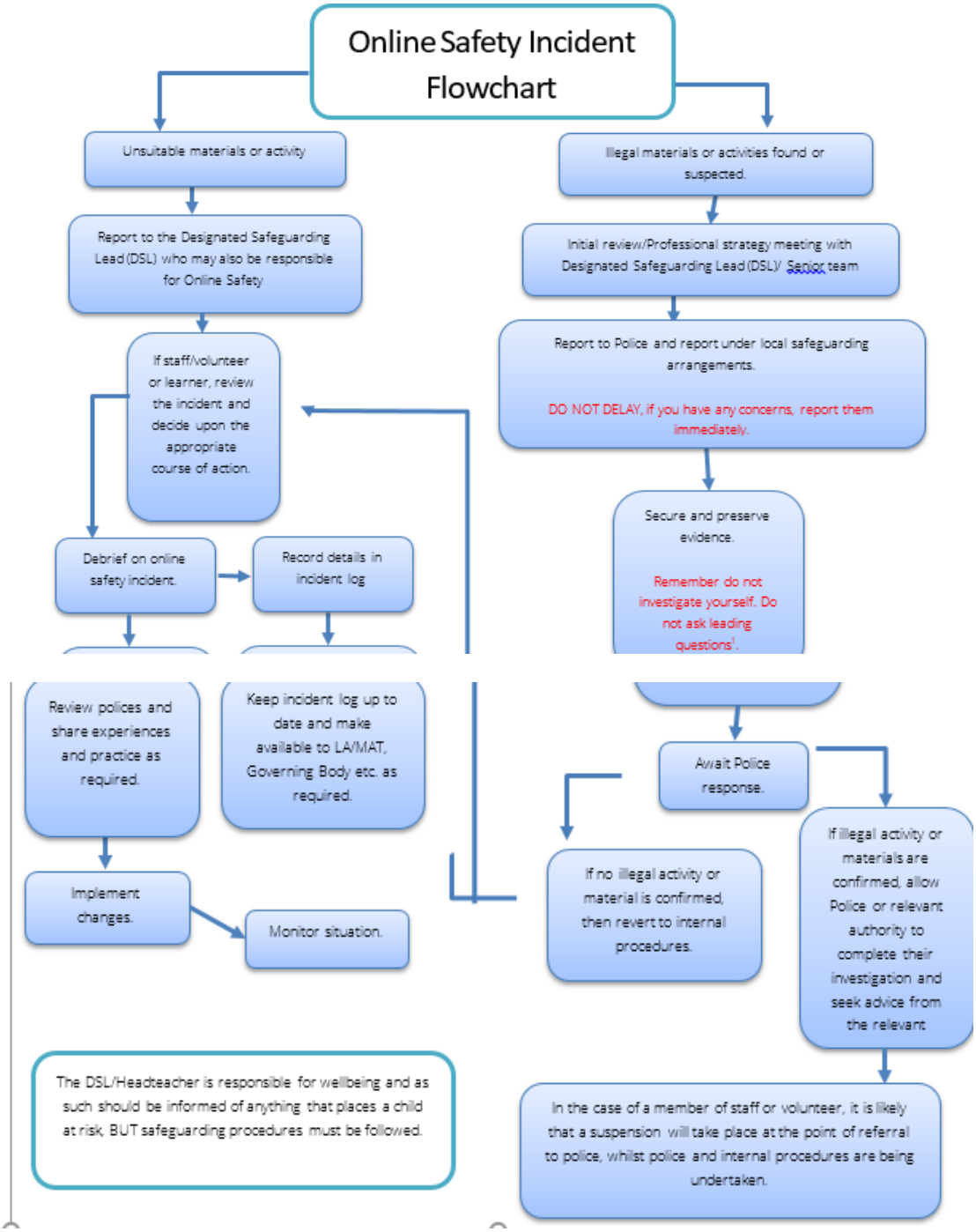
Actions where there are concerns about a child

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

Actions where there are concerns about a child



[1] In cases which also involve a concern or an allegation of abuse against a staff member, see Part four of this guidance.
[2] Early help means providing support as soon as a problem emerges at any point in a child's life. Where a child would benefit from co-ordinated early help, an early help inter-agency assessment should be arranged. Working Together to Safeguard Children provides detailed guidance on the early help process.
[3] Referrals should follow the process set out in the local threshold document and local protocol for assessment. See Working Together to Safeguard Children.
[4] Under the Children Act 1989, local authorities are required to provide services for children in need for the purposes of safeguarding and promoting their welfare. Children in need may be assessed under section 17 of the Children Act 1989. Under section 47 of the Children Act 1989, where a local authority has reasonable cause to suspect that a child is suffering or likely to suffer significant harm, it has a duty to make enquiries to decide whether to take action to safeguard or promote the child's welfare. Full details are in Working Together to Safeguard Children.
[5] This could include applying for an Emergency Protection Order (EPO).

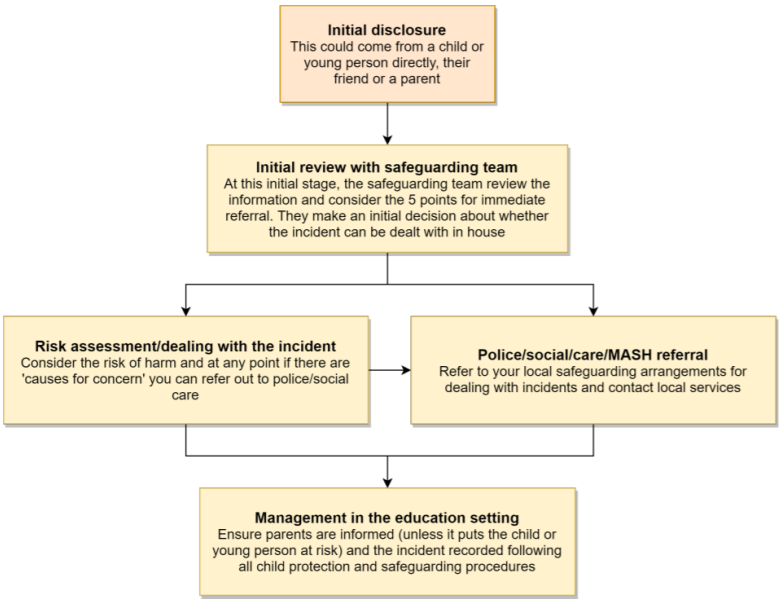

Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions!.
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Sharing nudes and semi-nudes

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on sexting - now referred to as Sharing nudes and semi-nudes: advice for education settings to avoid unnecessary criminalisation of children. 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 Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL 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, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.



***Consider the 5 points for immediate referral at initial review:**

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming

It is important that everyone understands that whilst sharing nudes and semi-nudes 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 documents referenced above and materials to support teaching about sexting can be found at sexting.lgfl.net

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/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

See Child Protection Policy

Bullying

Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

See anti-bullying policy

https://sheffieldscb.proceduresonline.com/p_bullying.html

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. All staff are aware of this guidance: part 5 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.

See Child Protection Policy

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

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff 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 absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the local 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 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, POSH, (run by the UK Safer Internet Centre) for support or help to accelerate this process.

Data protection and data security

GDPR information on the relationship between the school and LGfL can be found at gdpr.lgfl.net; there are useful links and documents to support schools with data protection in the 'Resources for Schools' section of that page.

There are references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education' and 'Data protection: a toolkit for schools' (August 2018), which the DPO and DSL will seek to apply. This quote from the latter document is useful for all staff – note the red and purple highlights:

"**GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe.** Lawful and secure information sharing between schools, Children's Social Care, and other local agencies, is essential for keeping children safe and ensuring they get the support they need. **The Data Protection Act 2018 introduced 'safeguarding' as a reason to be able to process sensitive, personal information, even without consent** (DPA, Part 2,18; Schedule 8, 4) When Designated Safeguarding Leads in schools are considering whether, or not, to share safeguarding information (especially with other agencies) **it is considered best practice for them to record who they are sharing that information with and for what reason. If they have taken a decision not to seek consent from the data subject and/or parent/carer that should also be recorded within the safeguarding file. All relevant information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children**."

All pupils, staff, governors, volunteers, contractors and parents are bound by the school's data protection policy and agreements.

Rigorous controls on the network, USO sign-on for technical services, firewalls and filtering all support data protection.

The Executive headteacher, data protection officer and governors work together to ensure a GDPR-compliant framework for storing data, but which ensures that child protection is always put first and data-protection processes support careful and legal sharing of information.

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions.

Appropriate filtering and monitoring

Technology

The DfE Filtering and Monitoring Standards states that "Your IT service provider may be a staff technician or an external service provider". If the school has an external technology provider, it is the responsibility of the school to ensure that the provider carries out all the online safety and security measures that would otherwise be the responsibility of the school. It is also important that the technology provider is fully aware of the school Online Safety Policy/acceptable use agreements and the school has a Data Processing Agreement in place with them. The school should also check their local authority/other relevant body policies on these technical and data protection issues if the service is not provided by

the authority and will need to ensure that they have completed a Data Protection Impact Assessment (DPIA) for this contract.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

Filtering & Monitoring

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states: "It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place …governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified…

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider (Blue Box) and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL will have lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility

The filtering and monitoring provision is reviewed annually by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of Blue Box.

- checks on the filtering and monitoring system are carried out by Blue Box IT with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified, there is a change in working practice,
- A Smoothwall report is received weekly (along with instant notifications of breeches) to highlight any breaches. Hannah Travers and Helen Fenlon analyse the report. Any incidents are investigated/ addressed by the Online Safety lead/DSL.

Filtering

- the school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.
- illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective
- there is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are reviewed and the Designated Safeguarding Lead is alerted to breaches of the filtering policy, which are then acted upon.
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different abilities/ages/stages and different groups of users: staff/learners, etc.)
- younger learners will use child friendly/age-appropriate search engines
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Smoothwall monitoring reports are reviewed weekly, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

Monitoring includes

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed (Smoothwall reports)
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems

See below for Flowchart of internet breach incident and sanctions (pupils and staff)

Flowchart of internet breach incident and sanctions (pupils)

These actions are applied to breaches identified through Smoothwall and breaches identified by pupils.

Each breach will be investigated and consequences will be proportionate up to and including suspension/exclusion from the school on a temporary or permanent basis"

Breach identified

Red (danger)	Yellow (caution)	Blue (advisory)
Possible actions- Report to online safety officers Meeting with child Inform parents/carers Sanctions Report on CPOMS Whole class follow up lessons Contact Safeguarding	**Possible Actions –** Report to online safety officers Meeting with child Inform parents/carers Sanctions Report on CPOMS Whole class follow up lessons	**Possible Actions –** Report to online safety officers Meeting with child Inform parents/carers Sanctions Whole class follow up lessons

Flowchart of internet breach incident and sanctions (Staff)

Each breach will be investigated and consequences will be proportionate to that breach

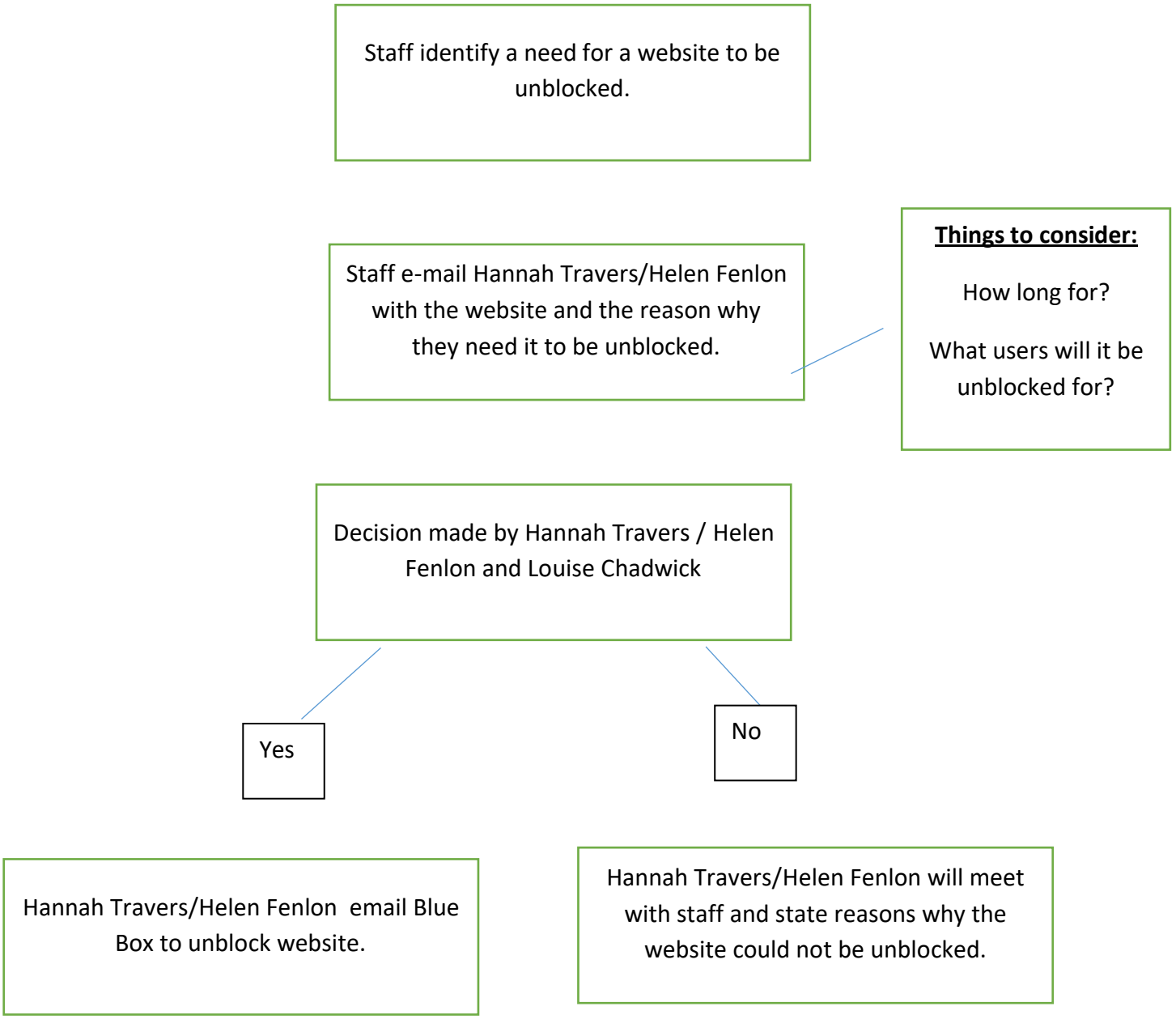
Breach identified

Red (danger)	Yellow (caution)	Blue (advisory)
Possible actions- Report to online safety officers Meeting with senior leaders School support-counselling Contact safe guarding advisory desk Disciplinary Staff allegation procedure Criminal action	**Possible Actions –** Report to online safety officers Meeting with senior leaders Staff training School support-counselling	**Possible Actions –** Report to online safety officers Meeting with senior leaders

Website **blocking** procedure

If staff want to block a website then they must email Hannah Travers with the website that that require to be blocked. In the email staff must give the reasons why they want the website blocked.

Website **unblocking** procedure



Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements :

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the IT service provider and will be reviewed, at least annually, by the SLT
- password policy and procedures are implemented. (consistent with guidance from the National Cyber Security Centre)
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- appropriate security measures are in place (schools may wish to provide more detail which may need to be provided by the service provider) to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- Zoe Clarke/Lisa Hoffman is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)

- use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/Blue Box
- removable media is not permitted unless approved by the SLT/IT service provider
- systems are in place to control and protect personal data and data is encrypted at rest and in transit. (See school personal data policy template in the appendix for further detail)
- mobile device security and management procedures are in place (where mobile devices are allowed access to school systems). (Schools may wish to add details of the mobile device security procedures that are in use).
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Electronic communications

Email

- Staff at this school use office 365 system for all school emails

These systems are linked to the USO authentication system and are fully auditable, trackable and managed on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents, as well as to support data protection.

General principles for email use are as follows:

- Email, Class Dojo, Google Classroom and tapestry (FS only) is the only means of electronic communication to be used between staff and pupils / staff and parents (in both directions). Use of a different platform must be approved in advance by the data-protection officer / headteacher in advance. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
- Email may only be sent using the email systems above. There should be no circumstances where a private email is used; if this happens by mistake, the DSL/Headteacher/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.
- Staff or pupil personal data should never be sent/shared/stored on email.

- If data needs to be shared with external agencies, staff should use AnyComs or speak to DSL/OSL
- Internally, staff should use the school network, including when working from home

- 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

School website

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher and Governors have delegated the day-to-day responsibility of updating the content of the website to Hannah Travers/Tracy Lilley/Sarah Short. The site is managed by / hosted by EDHQ

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 Dee Whitmore. There are many open-access libraries of high-quality public-domain images that can be used (e.g. pixabay.com for marketing materials – beware some adult content on this site).
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Cloud platforms

It is important to consider data protection before adopting a cloud platform or service

For online safety, basic rules of good password hygiene ("Treat your password like your toothbrush –never share it with anyone!"), expert administration and training can help to keep staff and pupils safe, and to avoid incidents. The data protection officer and network manager Bluebox IT analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- Privacy statements inform parents 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 parental permission is sought

- Regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- Pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- Two-factor authentication is used for access to staff or pupil data
- Pupil images/videos are only made public with parental permission
- Only school-approved platforms are used by students or staff to store pupil work
- All stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain)

Digital images and video

When a pupil/student 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.

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.

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 Ecclesfield and Coit Primary no member of staff will ever use their personal phone to capture photos or videos of pupils.**

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

Staff and parents are reminded annually about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. Further detail on this subject and a sample letter to parents for taking photos or videos at school events can be found at parentfilming.lgfl.net

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.

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

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.

Staff, pupils' and parents' 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, staff and pupils will use it. However, 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 the teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

If parents have a concern about the school, we would urge them to contact us directly 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 but the school regularly deals with issues arising on social media with pupils/students 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/students 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.

Email is the official electronic communication channel between parents and the school.

Pupils/students/parents/carers are discouraged from attempting to 'follow' staff, governor, volunteer or contractor social media accounts. In the reverse situation, staff must not follow student or parental social media accounts.

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, trust or local authority, bringing the school into disrepute.

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. Permission is sought before uploading photographs, videos or any other information about other people.

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

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video section. 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. for contractors to take photos of equipment or buildings), permission of the headteacher should be sought (the headteacher may choose to delegate this) and this should be done in the presence of a member staff.
- **Parents** are asked to leave their phones in their pockets and turned off when they are on site. They should ask permission before taking any photos, e.g. of displays in corridors or classrooms, and avoid capturing other children. When at school events, please refer to the Digital images and video section of this document on page . Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office. (see parental code of conduct)

Network / internet access on school devices

- **Pupils/students** are not allowed networked file access via personal devices.

- **All staff who work directly with children** should leave their mobile phones on silent and only use them in private staff areas during school hours. See also the Digital images and video
- Child/staff data should never be downloaded onto a private phone.
- **Volunteers, contractors, governors** have no access to the school network or wireless internet on personal devices can access the guest wireless network but have no access to networked files/drives, subject to the acceptable use policy. All internet traffic is monitored.
- **Parents** have no access to the school network or wireless internet on personal devices

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

Searching and confiscation

In line with the DfE guidance '[Searching, screening and confiscation: advice for schools]', the Headteacher/Principal 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.

Appendices

APPENDIX 1: Example Acceptable Use Policies

For KS1 and FS classes the following Acceptable Use Policy will be discussed and agreed to by all members of the class

Ecclesfield Primary School

Online Safety Acceptable Use Policy Foundation Stage and KS1

Coit Primary School

I will only use the Internet with an adult or when I have asked for an adult's permission.

I will only click on games, APPS, images and websites that I know are safe and when I have had permission from a trusted adult.

I will only send polite and friendly messages to people that I know. If I receive an unfriendly message, then I will tell an adult and keep a copy of it for evidence.

If I see something that I don't like online or if something makes me feel uncomfortable, I will always tell an adult that I trust straightaway.

I know that I need to spend time off line to enjoy a healthy and active lifestyle.

I will not reveal personal information online and will keep information such as my address, phone number and full name confidential.

I will think of a secure password and I won't share it. I won't share other people's passwords or ask them for it.

Signed by Y

For KS2 classes the following Acceptable Use Policy will be discussed and agreed to by all members of the class

Ecclesfield Primary School

Online Safety Acceptable Use Agreement
KS2

Coit Primary School

This acceptable use agreement is intended:

- to ensure that learners will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help learners understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password (or any other personal details) with anyone or try to use any other person's username and password.
- I will communicate and collaborate online with people I already know and have met in real life or that a trusted adult knows about.
- I know new online friends might not be who they say they are – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line. I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.

I understand that everyone has equal rights to use technology to support our education:

- I understand that the school ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so. I will only visit sites that adults have told me are safe.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.
- I know just calling something banter doesn't make it ok as it could become bullying. I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.

I understand that the school has a responsibility to keep the technology secure and safe:

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.
- I will only use chat and social networking sites with permission and at the times that are allowed

When using the internet for research for my school work, I understand that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I find is accurate, as I understand that the work of others may not be correct.
- I understand that the school will monitor my use of the internet.
- I will not make any attempt to bypass the filtering settings provided in school.

I understand that I am responsible for my actions, both in and out of school:

- I behave the same way on devices as face to face in the classroom, and so do my teachers – If I get asked to do anything that I would find strange in school, I will tell a teacher.
- I understand that the school could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of school as well as in school. Examples of this are online bullying, sending/receiving inappropriate images and misuse of personal information.
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to further action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment out of school in a way that is related to me being a member of this school eg communicating with other members of the school e.g. through social networks, mobile phones, accessing school email, Learning Platform, website etc.
- I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.

My trusted adults are:

Name of Student / Pupil ……

Signed …… Date ……

- STAF AUP

Staff ICT Acceptable Use Policy

2024-2025

All staff (including support staff), governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the school's approaches, strategy and policy as detailed in the full Online Safety Policy.

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

We ask all children, young people and adults involved in the life of Ecclesfield and Coit Primary School to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- I have read and understood Ecclesfield and Coit Primary School's full Online Safety policy and agree to uphold the spirit and letter of the approaches outlined there, both for my behaviour as an adult and enforcing the rules for pupils/students. I will report any breaches or suspicions (by adults or children) in line with the policy without delay.
- I understand that Information Systems include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites.
- School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988/2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the online safety policy and will always take into account parental consent.

- I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform (Sharepoint) to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information. I will never use school devices and networks/internet/platforms/other technologies to access material that is illegal or in any way inappropriate for an education setting. I will not attempt to bypass security or monitoring and will look after devices loaned to me.

- I will not support or promote extremist organisations, messages or individuals, nor give them a voice or opportunity to visit the school. I will not browse, download or send material that is considered offensive or of an extremist nature.

- I will respect copyright and intellectual property rights.

- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Joanne Eagleton – Coit / Hannah Travers – Ecclesfield) and/or the Online Safety Coordinator (Hannah Travers / Helen Fenlon) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Hannah Travers / Helen Fenlon) the Online Safety Coordinator

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team as soon as possible.

- My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number, class dojo, google Classroom, pre-arranged Zoom meetings. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- I understand the importance of upholding my online reputation, my professional reputation and that of the school), and I will do nothing to impair either.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the City Council, into disrepute.

- I understand the responsibilities listed for my role in the school's Online Safety policy. This includes promoting online safety as part of a whole school approach in line with the RSHE curriculum, as well as safeguarding considerations when supporting pupils remotely.

- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media, e.g. by:

- I understand I must not sharing other's images or details without permission

- I will refrain from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.

- If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Online Safety Coordinator (Hannah Travers/Helen Fenlon) or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

- I understand that breach of this AUP and/or of the school's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the school and where appropriate, referral to the relevant authorities.

Further guidance:

https://www.safeguardingsheffieldchildren.org/assets/1/online_safety___risk_assessment_sept_21.pdf

https://www.safeguardingsheffieldchildren.org/assets/1/photographs_video_s___images_sept_21.pdf

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood the Staff ICT Acceptable Use Policy.

Signed: …….... Print Name: …….... Date: ……

Accepted by: H.Travers …. Print Name: Hannah Travers

Parental AUP (New Starters)

Parent / Carer Acceptable Use Policy Agreement 2025-2026

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times. **Remote learning and online homework has become particularly important and highlights the importance of online technologies to support and enhance education.**

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour, **including remote learning and online homework.**

The school will try to ensure that *pupils* will have good access to ICT **and online home learning,** to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users.

As a school, we would hope that parents will share our mission to educate our pupils and therefore we ask parents to model appropriate behaviours on line and with new technologies. This in turn will support our pupils in becoming safe and responsible users of technology in this important aspect of the school's work.

We tell your children that they should not behave any differently when they are out of school or using their own device or home network. What we tell pupils about behaviour and respect applies to all members of the school community:

"Treat yourself and others with respect at all times; treat people in the same way when you are online or on a device as you would face to face."

When communicating with the school via official communication channels, or using independent channels to discuss issues pertaining to the school...

I will:

- Be respectful towards members of staff, and the school, at all times. **This includes when the children participate in remote learning sessions and when parents/carers attend remote sessions.**

- Be respectful of other parents/carers and children. **This includes when the children participate in remote learning sessions and when parents/carers attend remote sessions.**
- Endeavour to engage with relevant members of staff and if appropriate, the official complaints procedures, when seeking to raise a complaint with the school. **The school wishes to engage in constructive conversation with all stakeholders, and solely raising complaints on social media sites often undermines progress and disempowers the relationship between parents and the school.**
- Only upload or share photos or videos on social media of my own child/children.

Children at Ecclesfield Primary

I understand that Ecclesfield Primary uses technology as part of the daily life of the school when it is appropriate to support teaching & learning and the

smooth running of the school, and to help prepare the children and young people in our care for their future lives. I give permission for my child to have access to the internet and to ICT systems at school.

I know that my child has signed an Acceptable Use Agreement or has created their own and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I understand and support the commitments made by my child in the Acceptable Use Policy (AUP) which s/he has signed and I understand that s/he will be subject to sanctions if s/he does not follow these rules.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the school if I have concerns over my child's Online Safety.

The impact of social media use is often felt strongly in schools, which is why we expect certain behaviours from pupils when using social media. I will support the school's social media policy and not encourage my child to join any platform where they are below the minimum age.

Parent/Carer Signature_____

Pupil Name_____

Date_____