E-Safety policy

Trewirgie Infants' & Nursery School

Approved by:	LBG	**Date:** March 2025	
Next review due by:	February 2026		

Introduction

Key people / dates

	Designated Safeguarding Lead (DSL) team	DSL: Clair Bateman Deputy DSL: Cath Callow Vicky McKerron
	Online-safety lead (if different)	Clair Bateman
	Online-safety / safeguarding link LMC	Emma Guppy- Wilcox
	PSHE/RSHE lead (Jigsaw)	Clair Bateman
	Network manager / other technical support	TPAT Technical Support
	Date this policy was reviewed and by whom	- January 2025 C Jenkin
	Date of next review and by whom	January 2065 (Online Safety Team)

What is this policy?

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2022 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and other statutory documents. It complements existing and forthcoming subjects including Health, Relationships and Sex Education, Citizenship and Computing; it is designed to sit alongside our school's statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection procedures.

Who is it for; when is it reviewed?

This policy is a living document, subject to full annual review but also amended where necessary during the year in response to developments in the school and local area. The following policies will be reviewed every 12months. We recommend you read the **DfE** 'Get help with remote education' guidance at safepolicies.lgfl.net when reissuing your school policies for online safety, safeguarding and AUPs to see what needs changing in the light of potential closure, remote learning and alternative arrangements at school. Although many aspects will be informed by legislation and regulations, our staff, LMC members, pupils and parents are consulted and reviewing the policy (KCSIE stresses making use of teachers' day-to-day experience on the ground). This will help ensure all stakeholders understand the rules that are in place and why, and that the policy affects day-to-day practice. Pupils could help to design a version in language their peers understand or help you to audit compliance. Acceptable Use Policies (see appendices) for different stakeholders help with this – ensure these are reviewed alongside this overarching policy. Any changes to this policy should be immediately disseminated to all the above stakeholders.

Who is in charge of online safety?

Clair Bateman is our named online-safety lead at our school, as well as DSL.

What are the main online safety risks today?

Online-safety risks are traditionally categorised as one of the 3 Cs: Content, Contact or Conduct (identified by Professor Tanya Byron's 2008 report "Safer children in a digital world"). These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Many of these new risks are mentioned in KCSIE 2021, e.g. extra-familial harms where children are at risk of abuse or exploitation to multiple harms in situations outside their families including sexual exploitation, criminal exploitation, serious youth violence, upskirting and sticky design (making a website hard to leave once visited).

Following the government's investigation into **peer-on-peer sexual abuse** and Ofsted review, schools will need to review their policies to ensure appropriate processes are in place to allow pupils to report sexual harassment and abuse concerns freely, knowing these will be taken seriously and dealt with swiftly and appropriately.

How will this policy be communicated?

This policy will be communicated in the following ways:

- Posted on the school website
- Available on the internal staff network/drive
- Available in paper format in the staffroom
- Part of school induction pack for all new staff (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, LMC members, 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
- AUPs are displayed in appropriate classrooms/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

Overview

Aim

This policy aims to:

- Set out expectations for all Trewirgie Infant School community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, 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 at Trewirgie Infants' and Nursery School).

Further Help and Support

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy (reporting onto **MyConcern**). The DSL will handle referrals to local authority multi-agency safeguarding hubs (MARU) and normally the Headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Beyond this, **reporting.lgfl.net** has a list of curated links to external support and helplines for both pupils and staff, including the Professionals' Online-Safety Helpline from the UK Safer Internet Centre and the new NSPCC Report Abuse Helpline for sexual harassment or abuse, as well as hotlines for hate crime, terrorism and fraud which might be useful to share with parents, and anonymous support for children and young people.

Scope

This policy applies to all members of Trewirgie Infant School's community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, LMC members, 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.

Headteacher – Catherine Callow

Key responsibilities:

- Support safeguarding leads and technical staff as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see remotesafe.lgfl.net for policy guidance and an infographic overview of safeguarding considerations for remote teaching technology.
- Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding
- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships
- Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and LMC members to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures
- Ensure LMC members are regularly updated on the nature and effectiveness of the school's arrangements for online safety

- Ensure the school website meets statutory requirements (see appendices for website audit document)

- 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

Designated Safeguarding Lead / Online Safety Lead – Clair Bateman

Key responsibilities (remember the DSL can delegate certain online safety duties, e.g. to the online-safety coordinator, but not the overall responsibility; this assertion and all quotes below are from Keeping Children Safe in Education 2021):

- "The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection [including online safety] … this **lead** responsibility should not be delegated"
- Work with the HT and technical staff to review protections for pupils in the home where possible and as a minimum to make parents aware of their responsibilities and need to monitor content and usage of any devices used in the home. and remote-learning procedures.
- Where the online-safety coordinator is not the named DSL or deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised
- Ensure "An effective approach to online safety [that] empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate."
- "Liaise with staff (especially pastoral support staff, IT Technicians, and SENDCOs 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 LMC members 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." – see safetraining.lgfl.net and prevent.lgfl.net. Complete relevant training on the academy trust's Safesmart system. Prevent training took place January 2024 for all staff. Online safety training will be delivered through the Spring term during staff meetings and support staff during a KIT meeting.
- 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 LMC members/trustees.
- Receive regular updates in online safety issues and legislation, be aware of local and school trends.
- Ensure that online safety education is embedded across the curriculum in line with the statutory RSHE guidance (e.g. by use of the updated UKCIS framework 'Education for a Connected World – 2020 edition') and beyond, in wider school life
- Promote an awareness of and commitment to online safety throughout the school community, with a strong focus on parents, but also including hard-to-reach parents – dedicated resources at parentsafe.lgfl.net, monthly e-safety newsletter, School website and parent information meetings

(February 2024 and Summer term 2024).

- 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.
- Oversee and discuss 'appropriate filtering and monitoring' with LMC members and ensure staff are also aware. Are you talking to your technical teams? Whilst they will do the technical work, key decisions on what should be allowed are the responsibility of the DSL who should be careful to keep children safe.
- Ensure the updated 2021 DfE guidance on Sexual Violence & Sexual Harassment Between Children in Schools & Colleges Guidance is followed throughout the school and that staff adopt a zero-tolerance, whole school approach to this, as well as to bullying.
- Facilitate training and advice for all staff, including supply teachers:
    - all staff must read KCSIE Part 1 and all those working with children Annex B – translations are available in 12 community languages at kcsietranslate.lgfl.net
    - Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
    - All staff to be aware of Annex D (online safety)
    - cascade knowledge of risks and opportunities throughout the organisation
    - cpd.lgfl.net has helpful CPD materials including PowerPoints, videos and more
- DSL has had training in using the OnGuard managed system September 2023.

Governing Body, led by Online Safety / Safeguarding Link Governor – Mark Lees

Key responsibilities (quotes are taken from Keeping Children Safe in Education 2022)

- 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 (see remotesafe.lgfl.net for guidance to policies and an infographic overview of safeguarding considerations for remote teaching technology.
- "Ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of DSL [with] **lead responsibility** for safeguarding and child protection (including online safety) [with] the appropriate status and authority [and] time, funding, training, resources and support…"
- Support the school in encouraging parents and the wider community to become engaged in online safety activities

- Have regular strategic reviews with the online-safety coordinator / DSL and incorporate online safety into standing discussions of safeguarding at governor meetings
- Where the online-safety 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; this is completed via Smart log.
- "Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated annually in line with advice from local safeguarding partners and informed by KCSIE. Training is integrated, aligned and considered as part of the overarching safeguarding approach." There is further support for this at cpd.lgfl.net
- "Ensure that children are taught about safeguarding, including online safety [...] as part of providing a broad and balanced curriculum [...] Consider a whole school 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. At Trewirgie Infant School Online safety is taught in our computing skills progression (units 1:1 in Year 1 and 2:2 in Year 2 of Purple Mash), Safer internet day, who to talk to and who keeps us safe is taught through our Jigsaw (PSHE) curriculum.

All staff

Key responsibilities:

- Pay particular attention to safeguarding provisions for **home-learning** and **remote-teaching technologies** (see remotesafe.lgfl.net for an infographic overview of safeguarding considerations for remote teaching technology. There are further details in the staff AUP (Appendix 1).
- All staff to complete 'SafeSmart' E-Safety training.
- Recognise that **RHSE (Jigsaw)** is now statutory and that it is a whole-school subject requiring the support of all staff.
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up.
- Know who that Clair Bateman is the Designated Safeguarding Lead (DSL) and our Online Safety Lead (OSL).
- Read Part 1, Annex B and Annex D of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex B for SLT and those working directly with children, it is good practice for all staff to read all three sections). Annex A is now a condensed version of Part one and can be provided (instead of Part one) to those staff who do not directly work with children, if the governing body or proprietor think it will provide a better basis for those staff to promote the welfare and safeguard children.
- 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 (MyConcern).

- 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 (Appendix 1) and use in conjunction with the code of conduct and staff 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 **RHSE (Jigsaw)** 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). Staff to complete retrieval based tasks throughout the year revisiting E-Safety.
- 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). This is done through retrieval tasks throughout the year referencing the online safety unit which pupils have completed at the beginning of each year (for Years 1 and 2).
- When supporting pupils remotely, be mindful of additional safeguarding considerations – refer to the remotesafe.lgfl.net infographic which applies to all online learning.
- Carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking, age appropriate materials and signposting, and legal issues such as copyright and GDPR.
- Be aware of security best-practice at all times, including password hygiene 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 (Appendix 2 & 3)
- Notify the DSL/OSL of new trends and issues before they become a problem
- Take a zero-tolerance approach to bullying and sexual harassment (your DSL will disseminate relevant information from the updated 2021 DfE document on this)
- 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
- 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.

RHSE (Jigsaw) Lead/s – [Clair Bateman]

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Embed consent, mental wellbeing, healthy relationships and staying safe online into the 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 complements 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.
- RHSE policy is included on the school website.
- 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 – [Craig Jenkin]

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 RHSE 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 RHSE 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 – TPAT Technical Support

Key responsibilities:

- As listed in the 'all staff' section, plus:
- Support the HT and DSL team as they review protections for **pupils in the home** and **remote-learning** procedures, rules and safeguards (see remotesafe.lgfl.net for guidance to policies and

an infographic overview of safeguarding considerations for remote teaching technology.

- 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 RHSE 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
- Maintain up-to-date documentation of the school's online security and technical procedures
- To report online-safety related issues that come to their attention in line with school policy
- Manage the school's systems, networks and devices, according to a strict password policy, with systems in place for detection of misuse and malicious attack, with adequate protection, encryption and backup for data, including disaster recovery plans, and auditable access controls.
- Work with the Headteacher to ensure the school website meets statutory DfE requirements.

Data Protection Officer (DPO) – Sarah Howe and Catherine Callow (HT)

Key responsibilities:

- Be aware that of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education 2022' 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."
- Work with the DSL, headteacher and LMC members to ensure frameworks are in place for the protection of data and of safeguarding information sharing as outlined above.
- Ensure that all access to safeguarding data is limited as appropriate, and also monitored and audited

Volunteers and contractors (including tutors)

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:

- 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.
- 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.
- Understand the benefits/opportunities and risks/dangers of the online world and know who to talk to at school or outside school if there are problems.

Parents/carers

Key responsibilities:

- 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, LMC members, contractors, pupils or other parents/carers.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns

External groups including parent associations

Key responsibilities:

- Any external individual/organisation will sign an acceptable use policy prior to using technology or the internet within school
- Support the school in promoting online safety and data protection
- Model safe, responsible, respectful and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining

from posting negative, threatening or violent comments about others, including the school staff, volunteers, LMC members, contractors, pupils or other parents/carers

Education and curriculum

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

- RSHE- Relationships Health and Sex Education. This is taught through **Jigsaw**
- 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)

Whenever overseeing the use of technology for example, ipads, cameras, laptops, PurpleMash activities in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law. saferesources.lgfl.net has regularly updated theme-based resources, materials and signposting for teachers and parents.

At Trewirgie Infant School, we recognise that online safety and broader digital resilience must be thread throughout the curriculum.

Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and RHSE).

General concerns must be handled in the same way as any other safeguarding concern;
Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies:

- Safeguarding and Child Protection Policy
- Child on child Abuse Policy
- Anti-Bullying Policy
- Behaviour Policy
- Acceptable Use Policies
- Prevent Policy
- 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 by the end of the lesson.

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Marck Lees Mlees1979@gmail.com (Chair of LMC) and the LADO (Local Authority's Designated Officer) LADO@Cornwall.gov.uk / 01872 326536. Staff may also use the Whistleblowing Helpline 08000280285.

The school will actively seek support from other agencies as needed (i.e. the local authority, SWGFL, 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.

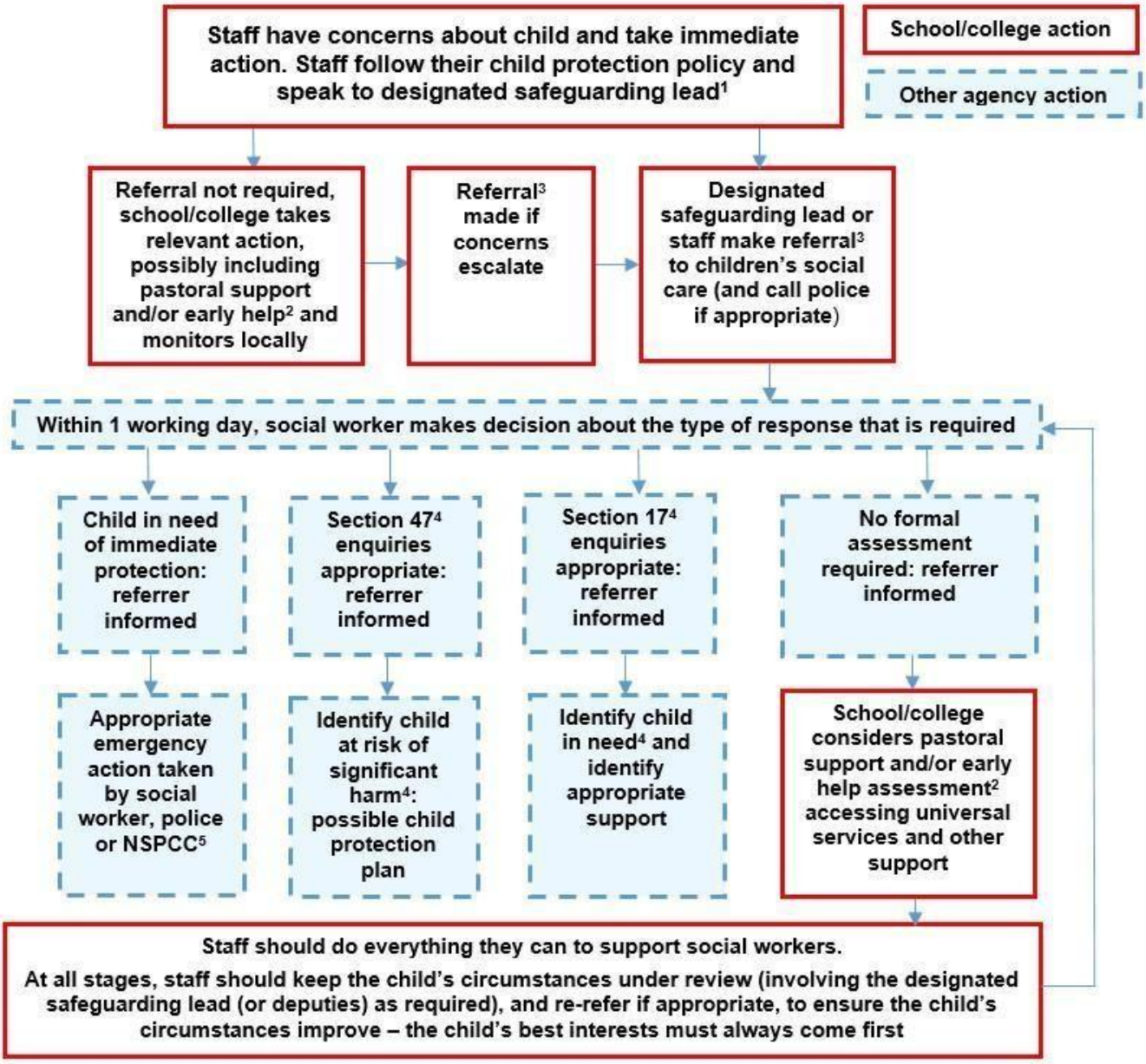
Communication with Parents

The School is adhering to the guidance within the revised KCSIE (September 2022) Paragraph 140- 142.

140. Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online. As a school we run Online Safety information sessions for parents, which are also uploaded onto our School website. Helpful advice and updates on the suitability of games and applications are on our monthly newsletter created by **Knowsley City Learning Centres**.

Actions where there are concerns about a child

The following flow chart is taken from page 22 of Keeping Children Safe in Education 2022 as the key education safeguarding document. As outlined previously, online safety concerns are no different to any other safeguarding concern.

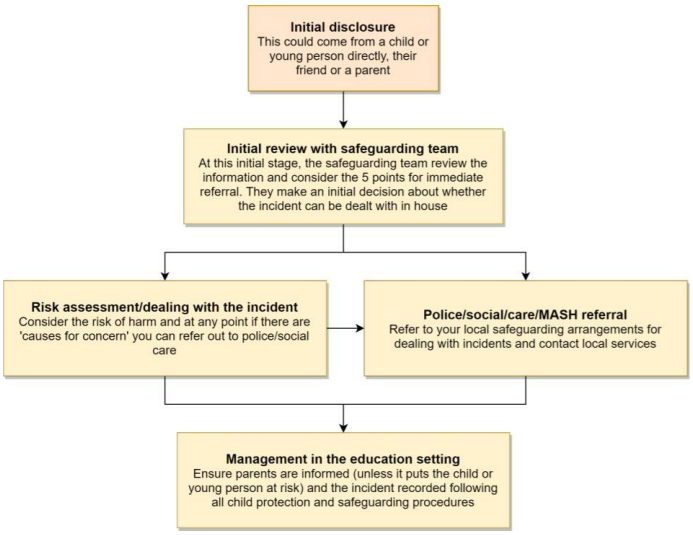

Staff have concerns about child and take immediate action. Staff follow their child protection policy and speak to designated safeguarding lead[1]
School/college action
Other agency action
Referral not required, school/college takes relevant action, possibly including pastoral support and/or early help[2] and monitors locally
Referral[3] made if concerns escalate
Designated safeguarding lead or staff make referral[3] to children's social care (and call police if appropriate)
Within 1 working day, social worker makes decision about the type of response that is required
Child in need of immediate protection: referrer informed
Section 47[4] enquiries appropriate: referrer informed
Section 17[4] enquiries appropriate: referrer informed
No formal assessment required: referrer informed
Appropriate emergency action taken by social worker, police or NSPCC[5]
Identify child at risk of significant harm[4]: possible child protection plan
Identify child in need[4] and identify appropriate support
School/college considers pastoral support and/or early help assessment[2] accessing universal services and other support
Staff should do everything they can to support social workers.
At all stages, staff should keep the child's circumstances under review (involving the designated safeguarding lead (or deputies) as required), and re-refer if appropriate, to ensure the child's circumstances improve – the child's best interests must always come first

Sexting – 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 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 sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

The 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.

Bullying

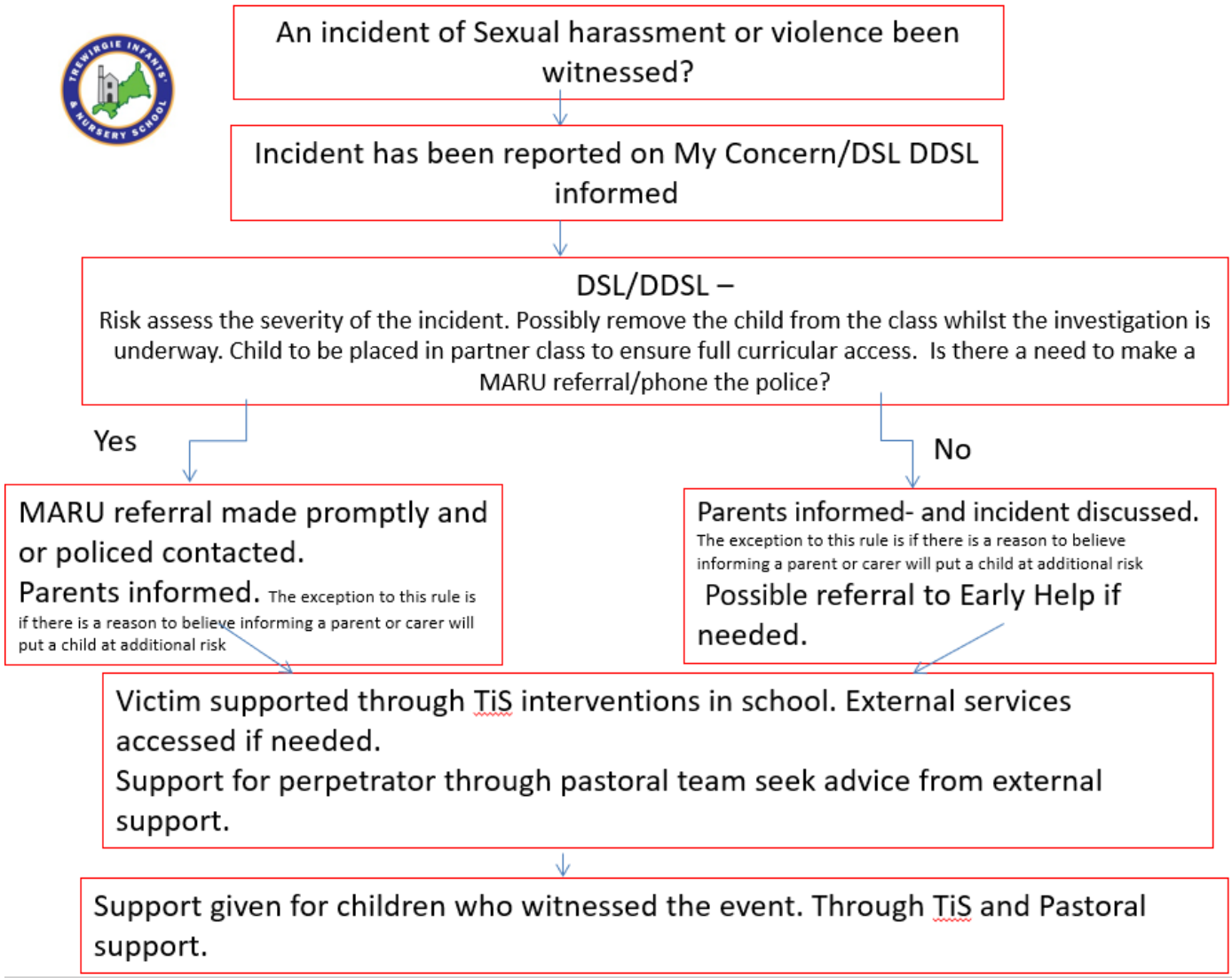
Online bullying should be treated like any other form of bullying and the school bullying policy should be followed for online bullying, which may also be referred to as cyberbullying, including issues arising from banter.

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

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. It would be useful for all staff to be aware of this guidance: paragraphs 45-49 cover the immediate response to a report and confidentiality which is highly relevant for all staff; the case studies section provides a helpful overview of some of the issues which may arise.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such the careless use of language. When we have incidents of this nature we follow the flow chart below.



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.

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.

Social media incidents

See the social media section later in this document for rules and expectations of behaviour for children and adults in the Trewirgie Infant School community. These are also governed by school Acceptable Use Policies.

Breaches will be dealt with in line with the school's Behaviour Policy or code of conduct/handbook (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

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, LMC members, volunteers, contractors and parents are bound by the school's and academy trust's data protection policy and agreements, which can be found HERE (trewirgie-inf.cornwall.sch.uk).

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

Staff are reminded that all safeguarding data is highly sensitive and should be treated with the strictest confidentiality at all times, and only shared via approved channels to colleagues or agencies with appropriate permissions. The use of Egress to encrypt all non-internal emails is compulsory for sharing pupil data, this will only be done by the Senior Leadership Team and the DPO and DSL will be informed in advance. All staff should contact Clair Bateman if they have been requested to send pupil data.

Appropriate filtering and monitoring

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material.

At this school, the internet connection is provided by SWGfL. This means we have a dedicated and secure, school-safe connection that is protected with a firewall and multiple layers of security from their network, including a web filtering system called RM SafetyNet, which is made specifically to protect children in schools. DSL has had training in using the OnGuard managed system.

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

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

Electronic communications

This section only covers electronic communications, but the same principles of transparency, appropriate conduct and audit trail apply.

Email

- Staff at this school use Outlook system for all school emails

General principles for email use are as follows:

- Class Dojo and via School email are the only means of electronic communication to be used between 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 the Egress system is available for use
    - Internally, staff should use the school network.
- 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

T

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 site is hosted by Eschools.

The DfE has determined information which must be available on a school website, this is checked regularly to ensure compliance.

At Trewirgie Infant School **Sarah Howe (Administration officer)** and **SLT** upload and update the school website.

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. 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).

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. Parents answer related to use on the following:

- For official school purposes of promoting or publicising school events e.g. newsletter
- For use on the school website
- For use in video recordings to promote the school
- For use in the school's own records, archives and future interest e.g. photographs of sports teams
- Consent that children can appear in video recordings or in collections of photographs stored on CD roms.
- Consent to be included in any images taken by other parents or carers who wish to photograph or record school events
- For use by the press
- For use on Class Dojo

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.

Any pupils shown in public facing materials are never identified with more than first name (and photo file names/tags do not include full names to avoid accidentally sharing them).

All staff are governed by their contract of employment 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 Trewirgie Infant School members of staff may occasionally use personal phones to capture photos or videos of pupils, but these will be appropriate, linked to school activities, taken without secrecy

and not in a one-to-one situation, and always moved to school storage as soon as possible, after which they are deleted from personal devices or cloud services (NB – many phones automatically back up photos).

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

Staff and parents are reminded regularly about the importance of not sharing without permission, due to reasons of child protection (e.g. looked-after children often have restrictions for their own protection), data protection, religious or cultural reasons, or simply for reasons of personal privacy. 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

Social media

Trewirgie Infant School's SM presence

Trewirgie Infant School works on the principle that if we don't manage our social media reputation, someone else will.

Online Reputation Management (ORM) is about understanding and managing our digital footprint (everything that can be seen or read about the school online). Few parents will apply for a school place without first 'googling' the school, and the Ofsted pre-inspection check includes monitoring what is being said online.

Negative coverage almost always causes some level of disruption. Up to half of all cases dealt with by the Professionals Online Safety Helpline (POSH: helpline@saferinternet.org.uk) involve schools' (and staff members') online reputation.

Accordingly, we manage and monitor our social media footprint carefully to know what is being said about the school and to respond to criticism and praise in a fair, responsible manner.

Cath Callow, Kirsten Maun and the **office staff** are responsible for managing our Facebook account.

Staff, pupils' and parents' SM presence

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

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

If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure should be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset

to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).

Many social media platforms have a minimum age of 13 (note that WhatsApp is 16+). We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that Online Harms regulation is likely to require more stringent age verification measures over the coming years.

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.

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

The school has an official Facebook page and Twitter account and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.

Email is the official electronic communication channel between parents and the school, and between staff and pupils, alongside the The Class Dojo platform.

Pupils/students are not allowed* to be 'friends' with or make a friend request** to any staff, LMC members,
volunteers and contractors or otherwise communicate via social media.

Pupils/students are discouraged from 'following' staff, governor, volunteer or contractor public accounts (e.g. following a staff member with a public Instagram account). However, we accept that this can be hard to control (but this highlights the need for staff to remain professional in their private lives). In the reverse situation, however, staff must not follow such public student accounts.

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

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

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

The serious consequences of inappropriate behaviour on social media are underlined by the fact that during the last 5 years, there have been 263 Prohibition Orders issued by the Teacher Regulation Agency to teaching staff that involved misuse of social media/technology.

All members of the school community are reminded that particularly in the context of social media, it is important to comply with the school policy on Digital Images and Video (see page 24) and permission is

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

The statements of the Acceptable Use Policies (AUPs) which all members of the school community have signed are also relevant to social media activity, as is the trusts Data Protection Policy.

Device usage

Remind those with access to school devices about rules on the misuse of school technology – devices used at home should be used just like if they were in full view of a teacher or colleague. Please read the following in conjunction with acceptable use policies and the following sections of this document which all impact upon device usage: copyright, data protection, social media, misuse of technology, and digital images and video.

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

- **All staff who work directly with children** should not have their mobile phone on their person. See also the Digital images and video section on page and Data protection and data security section on page. 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, ask for the message to be left with the school office or have their phone on them with the permission of the headteacher. Is Staff risk assessment for more detail.
- **Classroom volunteers,** should leave their phones in the locked classroom cupboard and turned off. Under no circumstances should they be used in the presence of children or to take photographs or videos.
- **Contractors** 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. See Contractors Risk Assessment for more detail.
- **LMC members** should leave their phones in the SLT Room. 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** know that taking pictures is not permitted. 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. Parents are asked not to call pupils on their mobile phones during the school day; urgent messages can be passed via the school office.

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 not have their mobile phones on their person. See also the Digital images and video section and Data protection and data security section.

Child/staff data should never be downloaded onto a private phone.

- **Volunteers, contractors, LMC members** 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.

Trips / events away from school

For school trips/events away from school, teachers will take their own mobile phone for use in case of an emergency. 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 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.

Appendix 1 – Trewirgie Infant School Acceptable Use - Staff, Volunteers and LMC members

	Name of school	**Trewirgie Infant School**
	AUP review date	**March 2025**
	Date of next review	**March 2026**
	Who reviewed this AUP?	**E-safety team – Craig Jenkin, Cath Callow, Clair Bateman**

Refers to the use of all digital technologies in school: i.e. **e-mail, internet, network resources,** VLE (Eschools), software, communication tools, **equipment and systems:**

- I will follow the e-safety policy (including for mobile and handheld devices).
- I will only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not share my passwords to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access e-mail / Internet / VLE(Eschools) / network or other school systems.
- I will ensure all documents, data etc., are printed, saved, accessed and deleted / shredded in accordance with the school's network / information security policy.
- I will use an encrypted/password protected memory storage device or TPAT Trust one drive to store any school documents (Teachers)
- I will not engage in any online activity that may compromise my professional responsibilities.

- I will only use the school approved e-mail system(s) / *communication systems* for any school business, including communication with parents.
- I will only use the school's approved systems: schoolemail/*SchoolComms/ DoJo/ Tapestry* to communicate with pupils, and will only do so for teaching & learning purposes.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or any filtering breach to the E-safety team.
- I will not download any software or resources from the internet that can compromise the network or is not adequately licensed, or which might allow me to bypass filtering and security systems.
- I will check copyright and not publish or distribute any work, including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not use my own personal digital cameras, camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff and will not store any such images or videos at home.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the school approved system *(e.g iPads).*
- I will follow the school's policy on use of mobile phones / devices at school.
- I will ensure that any private social networking sites / blogs, etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure, where used, that I know how to use any social networking sites / tools securely and appropriately, so as not to compromise my professional role.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities, and that I will notify the school of any "significant personal use", as defined by HM Revenue & Customs.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption/password, and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information that is held within the school's information management system will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will alert the school's DSL (Clair Bateman) or appropriate senior member of staff if I feel the behaviour of any child with regard to computing and E-safety may be a cause for concern. I will log this on My Concern.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the school's DSL or appropriate senior member of staff at the school.
- I understand that all internet usage and network usage can be logged, and that this information can be made available *to the Head / Safeguarding Lead* on their request.
- *Staff that have a teaching role only:* I will embed the school's e-safety / digital literacy curriculum into my teaching .

Acceptable Use Agreement Form: Staff, Volunteers, LMC members

User Signature

I agree to abide by all the points above.

I understand that I have a responsibility for my own and others' e-safeguarding and I undertake to be a 'safe and responsible digital technologies user'.

I understand that it is my responsibility to ensure that I remain up-to-date and that I read and understand
the school's most recent E-safety policies.

I understand that failure to comply with this agreement could lead to disciplinary action.

Signature ..... Date .....

Full Name.....(printed)

Job Title / Role .....

Authorised Signature (Head Teacher)

I approve this user to be set-up on the school systems relevant to their role.

Signature ..... Date.....

Full name: Cath Callow

Trewirgie Infant School Acceptable use policy

Think before you click	
S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on a screen, I will always tell an adult

Date: September 2024

Appendix 4– Device Loan Agreement

Device loan agreement for pupils

1. This agreement is between:

1) Trewirgie Infant School ("the School")

2) [ ] ("the parent" and "I")

And governs the use and care of devices assigned to the parent's child (the "Pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the School.

All issued equipment shall remain the sole property of the School and is governed by the School's policies.

1. The School is lending the Pupil a laptop ("the equipment") for the purpose of doing schoolwork during the COVID19 Lockdown, from home.
2. This agreement sets the conditions for taking a [Trewrigie Infant School laptop ("the equipment")] home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the Pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement, I agree to take full responsibility for the loan equipment issued to the Pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that the Pupil and I are responsible for the equipment at all times, whether on the School's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform the Headteacher at School and I acknowledge that I am responsible for the reasonable costs requested by the School to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the School when requested from the School in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

If the equipment is damaged, lost or stolen, and your child is eligible for pupil premium, contact David Hick Headteacher.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I am aware that the School monitors the Pupil's activity on this device.

I agree that my child will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages the School, or risks bringing the School into disrepute
- Causing intentional damage to ICT facilities or materials
- Making any hardware or software changes to the equipment without authorisation from the School IT Department
- Using inappropriate or offensive language

I accept that the School will sanction the Pupil, in line with our behaviour/discipline policy, if the Pupil engages in any of the above **at any time.**

4. Personal use

I agree that the Pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Do not share the equipment among family or friends
- Ensure the antivirus software is up to date

If I need help doing any of the above, I will contact the TPAT Central ICT Team on the email itsupport@tpacademytrust.org or ring them on 01872 613289 (Phone support is available between 8:30am and 3:30pm, Monday to Friday).

6. Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so.

I will ensure the return of the equipment to the School if the Pupil no longer attends the School.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

S	