OUR LADY OF LOURDES CATHOLIC PRIMARY SCHOOL

School **Curriculum Policy and Subject Guidance** for

Online Safety

(2023/24)

Designated Safeguarding Lead: Mrs Liz Kendall

Our School Vision:

"We want our school to be a safe, secure and exciting place to learn and grow in Christ. A place where children, staff, families and governors work closely together to answer Christ's call."

Our Catholic School community works with a Christian purpose:

- To promote an enthusiasm for enjoyment of learning
- To provide a broad and well balanced curriculum
- To challenge children to reach their full potential
- To learn about God and his creation
- To answer Christ's call through our love for each other
- To foster in children independence and a sense of responsibility

"For you are precious in my eyes"
(Isaiah 43)

Key People & Dates:

Our Lady of Lourdes Catholic Primary School	Designated Safeguarding Lead (DSL) team	**Mrs Elizabeth Kendall**
	Online-safety / safeguarding link governor	**Mr Edward Hart**
	PSHE/RSHE lead	**Mrs Alison Townley**
	Network manager / other technical support	**Ed-It**
	Date this policy was reviewed and by whom	**September 2023**
	Date of next review and by whom	**September 2024** (amendments to be made as required) **Mrs Liz Kendall**

AIMS:

Through the implementation of the Online-safety policy at Our Lady of Lourdes we aim for all children to learn to:

- Be responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- Have a good understanding of research skills
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- To know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying
- To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to school

We regard On-line safety as important because:

- We understand the responsibility to educate our pupils in e-safety issues; teaching them appropriate behaviours, giving them the skills to develop critical thinking enabling them to stay safe and legal whilst online, both in and outside of a school setting.

ROLES & RESPONSIBILITES:

Governing Body/Safeguarding Lead (Edward Hart)	**Key responsibilities (quotes are taken from Keeping Children Safe in Education 2019):** ○ 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 ○ "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 co-ordinator / 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 A; check that Annex C on Online Safety reflects practice in your school • Ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. • 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
Designated Safeguarding Lead/Online Safety Lead (Elizabeth Kendall)	**Key responsibilities**: o Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns o 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 o Stay up to date with the latest trends in online safety o 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. o Receive regular updates in online safety issues and legislation, be aware of local and school trends – see safeblog.lgfl.net for examples or sign up to the LGfL safeguarding newsletter o Ensure that online safety education is embedded across the curriculum (e.g. by use of the UKCIS framework 'Education for a Connected World') and beyond, in wider school life o Promote an awareness and commitment to online safety throughout the school community, with a strong focus on parents, who are often appreciative of school support in this area, but also including hard-to-reach parents o Liaise with school technical, pastoral, and support staff as appropriate o 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 o 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 o Oversee and discuss 'appropriate filtering and monitoring' with governors (is it physical or technical?) and ensure staff are aware (Ofsted inspectors have asked classroom teachers about this).

	○ Ensure the 2021 DfE guidance on sexual violence and harassment is followed throughout the school and that staff adopt a zero-tolerance approach to this, as well as to bullying ○ Facilitate training and advice for all staff: • all staff must read KCSIE Part 1 • it would also be advisable for all staff to be aware of Annex C (online safety) • cascade knowledge of risks and opportunities throughout school
Headteacher (Elizabeth Kendall)	**Key responsibilities**: ○ Foster a culture of safeguarding where online safety is fully integrated into whole-school safeguarding ○ Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported ○ Ensure that policies and procedures are followed by all staff ○ Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Local Safeguarding Partnerships ○ Liaise with the designated safeguarding lead on all online-safety issues which might arise and receive regular updates on school issues and broader policy and practice information ○ Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the DPO, DSL and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information ○ Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles ○ Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles ○ Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident ○ Ensure suitable risk assessments are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised ○ Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online-safety procedures ○ Ensure governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety ○ Ensure the school website meets statutory requirements
	Key responsibilities: ○ Understand that online safety is a core part of safeguarding; as such it is part of everyone's job – never think that someone else will pick it up

All Staff	○ Know who the Designated Safeguarding Lead (DSL) and Online Safety Lead (OSL) are – Mrs Liz Kendall ○ Read Part 1, Annex A and Annex C of Keeping Children Safe in Education (whilst Part 1 is statutory for all staff, Annex A for SLT and those working directly with children, it is good practice for all staff to read all three sections). ○ Read and follow this policy in conjunction with the school's main safeguarding policy ○ Record online-safety incidents 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, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils) ○ Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, 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) ○ To carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law ○ Prepare and check all online source and resources before using within the classroom ○ Encourage pupils/students to follow their acceptable use policy, remind them about it and enforce school sanctions ○ Notify the DSL/OSL of new trends and issues before they become a problem ○ Take a zero-tolerance approach to bullying and low-level sexual harassment (your DSL will disseminate relevant information from the new 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 safety 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.
PSHE/HRSE Subject Leader (Mrs Alison Townley)	**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.
Computing Subject Leader (Ms Naomi Powell)	**Key responsibilities:** ○ As listed in the 'all staff' section, plus: • Oversee the delivery of the online safety element of the Computing curriculum in accordance with the national curriculum • Work closely with the DSL/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
Network Manager (Ed-It)	**Key responsibilities:** ○ As listed in the 'all staff' section, plus: • Keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • Work closely with the designated safeguarding lead / online safety lead / data protection officer / LGfL 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 • Network managers/technicians at LGfL schools may want to ensure that you take advantage of the following solutions which are part of your package: Sophos Anti-Virus, Sophos Anti-Phish (from Sept 2019), Sophos InterceptX, Sophos Server Advance, Malware Bytes, Egress (from Sept 2019), Meraki Mobile Device Management and CloudReady/NeverWare. These solutions which are part of your package will help protect the network and users on it • 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 • Work with the Headteacher to ensure the school website meets statutory DfE requirements (see appendices for website audit document)
Children	**Key responsibilities:** o Read, understand, sign and adhere to the student/pupil acceptable use policy and review this annually o Understand the importance of reporting abuse, misuse or access to inappropriate materials o Know what action to take if they or someone they know feels worried or vulnerable when using online technology o 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 o 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:** o Read, sign and promote the school's parental acceptable use policy (AUP) and read the pupil AUP and encourage their children to follow it o Consult with the school if they have any concerns about their children's and others' use of technology

	○ Promote positive online safety and model safe, responsible and positive behaviours in their own use of technology, including on social media: not sharing other's images or details without permission and refraining from posting negative, threatening or violent comments about others, including the school staff, volunteers, governors, contractors, pupils or other parents/carers. ○ NB: the LGfL DigiSafe survey of 40,000 primary and secondary pupils found that 73% of pupils trust their parents on online safety (but only half talk about it with them more than once a year).

CURRICULUM:

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

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

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for children).

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what children 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 children when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. We must demonstrate that we provide the necessary safeguards to help ensure that we have done everything that could reasonably be expected of us to manage and reduce these risks.

Handling On-line Safety Concerns and Incidents:

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship.
General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety 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 on pupils when they come into school. All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

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

Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant 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, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline, 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).

Sexting:

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

There is a one-page overview called Sexting; how to respond to an incident for all staff (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.

Upskirting:

It is important that everyone understands that upskirting (taking a photo of someone under their clothing) 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. Materials to support teaching about bullying and useful Department for Education guidance and case studies are at bullying.lgfl.net

Sexual Violence & Harrassment:

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 as bra-strap flicking and the careless use of language.

Misuse of School Technology:

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology.

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

Data Protection:

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.

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

Appropriate Filtering & Monitoring:

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place [and] not be able to access harmful or inappropriate material [but at the same time] be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

At this school, the internet connection is provided by BT Lancashire. This means we have a dedicated and secure, school safe connection that is protected with firewalls and multiple layers of security.

Email & Online Collaboration:

- Children may only use approved email accounts on the school system
- Children must immediately tell a teacher if they receive offensive messages
- Children must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Children may must not access others pupil's accounts or files
- Whole class or group email addresses should be used in school
- Children must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Children must not deliberately seek out offensive materials. Should any children encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.
- Children are expected not to use any rude or offensive language in their email communications, and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- Children must ask permission before accessing the internet and have a clear idea of why they are using it
- Computers and school laptops should only be used for school work and homework unless permission has been given otherwise.
- No program files may be downloaded from the internet to the computer, to prevent corruption of data and to avoid viruses
- Children must not bring in USBs from home for use in school without permission. This is for both legal and security reasons. USBs should be virus scanned before use.
- Access in school to external personal email accounts may be blocked
- The forwarding of chain letters is not permitted

Social Networking:

- At Our Lady of Lourdes, we block/filter access to social networking sites and newsgroups unless a specific use is approved

- Children are advised never to give out personal details of any kind which may identify them or their location
- Children are advised not to place personal photos on any social network space
- Children are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Children are encouraged to invite known friends only and deny access to others
- Children and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube or Instagram is 13 years old

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 all staff. The site is managed by Primary Site (Juniper).

The DfE has determined information which must be available on a school website.

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

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches. Sources must always be credited and material only used with permission.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published (remember also not to save images with a filename that includes a pupil's full name).

Digital media:

When a child 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 as follows:

- For displays around the school
- For the newsletter
- For use in paper-based school marketing
- For online prospectus or websites
- For social media

Any pupils shown in public facing materials are never identified with more than first name. 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 Our Lady of Lourdes 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.

School Trips & Events away from school:

For school trips/events away from school, teachers will be issued a school duty phone and this number used for any authorised or emergency communications with pupils/students and parents. Any deviation from this policy (e.g. by mistake or because the school phone will not work) will be notified immediately to the headteacher. Teachers using their personal phone in an emergency will ensure that the number is hidden to avoid a parent or student accessing a teacher's private phone number.

Links with other policies:

This policy links to the following policies and procedures:

- Computing policy
- Safeguarding & Child protection policy
- Anti-bullying policy
- Behaviour Management policy
- Equality information and objectives

Policy Date:	September 2023
Policy Review Date:	September 2024
Signed & Dated:	**Chair of Governors**
Signed & Dated:	**Headteacher** **Curriculum Leader**

Appendix A