Online Safety Policy

September 2023

Designated Safeguarding Lead: Jill Talbot (Headteacher)

Named Governor with lead responsibility: Rachael Dray (Safeguarding Governor)

Approved by the Governing Body Strategy Group 11/10/23

This Policy is due for renewal in Term 1

2024-25

ONLINE SAFETY POLICY

OF

GODINTON PRIMARY SCHOOL

SECTION ONE: AIMS AND POLICY SCOPE

1.1 Aims

1.1.1 This online safety policy has been written by Godinton Primary School involving staff, pupils and parents/carers, building on the Education People's mobile and smart technology policy template with specialist guidance and input as required.

1.1.2 It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, Early Years and Foundation Stage 2021 'Working Together to Safeguard Children' 2018, 'Behaviour in Schools: Advice for Headteachers and school staff' 2022, 'Searching, screening and confiscation at school' 2022 and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.

1.1.3 The purpose of the Godinton Primary Online Safety Policy is to:

- Ensure that all those within our school community are clear in their understanding that online safety is an essential part of safeguarding and acknowledges the school's duty to ensure that all children and staff are protected from potential harm when working online and using mobile and smart technology.
- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that Godinton Primary School is a safe and secure environment.
- Raise awareness with all members of Godinton Primary School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

1.1.4 This policy applies to all access to and use of online means of activity on site, including all mobile and smart technology; this includes mobile phones and personal devices such as tablets, e-readers, games consoles and wearable technology, such as 'smart watches and fitness trackers, which facilitate communication or have the capability to record sound and/or images. It also applies where learners, staff or other individuals have been provided with

setting issued devices for use, both on and off-site.

This policy applies to children, parents/carers and all staff, including the Governing Body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy).

1.2 Scope

- Godinton Primary School has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions. Godinton Primary School also identifies that online safety is an essential part of safeguarding and with this there is a clear duty to ensure that children are protected from potential harm online.
- Godinton Primary identifies that the internet and associated devices, such as computers, tablets, mobile phones wearable technology and games consoles are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks.
- Godinton Primary will empower our children to acquire the knowledge needed to use the internet and mobile and smart technology in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks.

Godinton Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material
- Contact: being subjected to harmful online interaction with other users
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

This policy must be read in conjunction with other relevant school policies including (but not limited to):

- Anti-bullying Policy
- Acceptable Use Policy
- Behaviour and Discipline Policy
- Photographic Images of Children Policy
- Child Protection (Safeguarding) Policy

- Staff Code of Conduct Policy
- Confidentiality Policy
- Curriculum Policies such as Personal, Social and Health Education (PSHE),Computing, Relationship and Sex Education (RSE)
- Cyber Security Response Plan
- GDPR

The School has appointed a member of the Governing Body to take lead responsibility for safeguarding including online safety; this is the Governor for Safeguarding, Rachael Dray.

1.2.1 Key responsibilities of the school community

The Designated Safeguarding Lead (DSL) (Jill Talbot – Headteacher) has lead responsibility for online safety.

Godinton Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

Key responsibilities of the Governing Body are:

To monitor the school's online safety programme, ensuring that:

- There is a whole school approach to online safety as referred to in KCSIE 2023 and the DfE non statutory guidance Teaching Online Safety in Schools.
- The school is teaching all children how to stay safe online, with adaptations being made for vulnerable children, victims of abuse and pupils with special educational needs and disabilities
- The designated safeguarding lead (DSL) takes responsibility for understanding the filtering and monitoring systems and processes in place as part of their role
- All staff undergo safeguarding and child protection training which includes online safety
- All staff understand their expectations, roles and responsibilities around filtering and monitoring as part of their safeguarding training
- The school's child protection policy includes how your school approaches filtering and monitoring on school devices and school networks
- Online safety is a running and interrelated theme within a whole school approach to safeguarding and related policies/procedures. This includes how online safety is addressed through all areas of school life, including the curriculum, school ethos, environment and parental responsibility
- The school has appropriate filtering and monitoring systems in place to protect pupils when they access the internet at school.
- The school does all it reasonably can to protect children from harmful content, contact conduct and commerce.

- The school takes care that its filtering and monitoring systems do not place unreasonable restrictions on what children can be taught regarding online teaching and safeguarding, according to KCSIE 2023 (paragraph 134).

Key responsibilities of the Senior Management Team are:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community.
- Ensuring that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Implement appropriate and up-to-date policies regarding online safety, which addresses the acceptable use of technology, peer on peer abuse, use of social media and mobile technology.
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- Undertake appropriate risk assessments regarding the safe use of technology on site.
- Work with technical staff / Towers IT support to ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content (including extremist material).
- Ensuring that the filtering and school network system is actively monitored. Taking responsibility for online safety incidents and liaising with external agencies as appropriate. Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice.
- Support the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities.
- Ensure robust reporting channels are in place for the whole community to access. regarding online safety concerns.
- Support staff to ensure that online safety is embedded within a progressive whole setting curriculum, which enables all learners to develop an appropriate understanding of online safety. Making appropriate resources available to support the development of an online safety culture.
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- Ensuring compliance with the filtering and monitoring expectations of KCSIE 2023.

Key responsibilities of the Designated Safeguarding/Online Safety Lead are:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented.
- Keeping up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Accessing regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Accessing regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Ensuring all members of staff receive regular, up-to-date and appropriate online safety training.
- Working with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day
- Ensuring that online safety is promoted to parents, carers, and the wider community through a variety of channels and approaches.
- Work with the school lead for data protection to ensure that practice is in line with legislation.
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- Monitor online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Governing Body and other agencies as appropriate.
- Liaising with the local authority and other local and national bodies as appropriate.
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other procedures on a regular basis (at least annually).
- Ensuring that online safety is integrated with other appropriate school policies and procedures.
- Meeting with the governor with a lead responsibility for safeguarding and online safety in order to update.
- Taking lead responsibility for understanding the filtering and monitoring systems and processes in place and ensuring that these are compliant with the expectations of KCSIE 2023.

Key responsibilities of staff are:

- Contributing to the development of online safety policies.

- Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- Taking responsibility for the security of setting systems and the data they use or have access to.
- Having an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Modelling good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embedding online safety education in curriculum delivery wherever possible.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- Take personal responsibility for professional development in this area.

Additional responsibilities of the IT Support Team:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering procedures are applied and updated on a regular basis; responsibility for its implementation is shared with the SMT.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the SMT.
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

- **Key responsibilities of pupils (at a level that is appropriate to their individual age, ability and vulnerabilities) are:**

- Engaging in age appropriate online safety education opportunities.
- Contributing to the development of online safety policies.
- Understanding the school's online safety rules and adhering to them.
- Respecting the feelings and rights of others both on and offline.
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.
- Taking responsibility for keeping themselves and others safe online.

Key responsibilities of parents and carers are:

- Reading the school/setting Acceptable Use Policies, encouraging their children to adhere to them, and adhering to them themselves where appropriate.
- Discussing online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home.
- Role modelling safe and appropriate uses of new and emerging technology.
- Identifying changes in behaviour that could indicate that their child is at risk of harm online.
- Seeking help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns.
- Using school systems, such as learning platforms, and other network resources, safely and appropriately.
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

SECTION TWO: EDUCATION AND ENGAGEMENT APPROACHES

2.1 Education and Engagement with Learners

Godinton Primary School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst children by:

- Ensuring education regarding safe and responsible use precedes internet access.
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and the computing curriculum.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating children in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching children to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Preparing them to identify possible online risks and to make informed decisions about how to act and respond.
- Ensuring they know how and when to seek support if they are concerned or upset by something they see or experience online.

Godinton Primary School will support children to read and understand the acceptable use policies in a way which suits their age and ability by:

- Sending acceptable usage agreements home
- Displaying acceptable use posters in all rooms with internet access.
- Informing children that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking pupil voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate

2.2 Education and Engagement with Vulnerable Learners

Godinton Primary School recognises that some children are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Godinton Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners if needed.

When implementing an appropriate online safety policy and curriculum our school will seek input from specialist staff as appropriate, for example the SENCO, Child in Care Designated Teacher.

2.3 Engagement and education of staff

- The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of the school' safeguarding practice. Online safeguarding will be addressed in the annual safeguarding updates for staff and in the schools programme of safeguarding training in accordance with statutory requirements.
- This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- To protect all staff and pupils, the school will implement Acceptable Use Policies which highlight appropriate online conduct and communication.
- Staff will be made aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff on a regular basis.

- Clear procedures for reporting issues or concerns to the Towers IT support team and to the DSL, are in place.
- The school will highlight useful online tools which staff should use with children in the classroom. These tools will vary according to the age and ability of the pupils.
- All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

2.4 Engagement and education of parents and carers

- The school recognises that parents/carers have an essential role to play in enabling children to become safe and responsible users of the internet and digital technology.
- Parents' attention will be drawn to the school Online Safety Policy and expectations in newsletters, letters, the school prospectus and on the school website.
- A partnership approach to online safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use or highlighting online safety at other well-attended events e.g. parent evenings, transition events, fetes and sports days.
- Parents will be requested to read online safety information as part of the Home School Agreement.
- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss its implications with their children.
- Information and guidance for parents on online safety will be made available to parents in a variety of formats.
- Parents will be encouraged to role model positive behaviour for their children online.
- Parents will be contacted if the school becomes concerned about a child's online activity.

SECTION THREE: REDUCING ONLINE RISKS

Godinton Primary School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

3.1 Technology within the classroom

Godinton Primary uses a wide range of technology. This includes access to:

- Computers, ipads, laptops and other digital devices and smart technology
- Internet which may include search engines and educational websites
- Apps
- Email

- Online games and games-based technologies
- Digital cameras and video cameras

Only staff have access to download free apps, any paid apps need to be installed by the Towers IT support.

3.2 Reducing Online Risks

The school's approach to filtering and monitoring is informed by the UK Safer Internet Centre guidance on appropriate filtering and monitoring and the filtering and monitoring standards document produced by the DfE which sets out that school's should:

Identify and assign roles and responsibilities to manage filtering and monitoring systems.

- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

Godinton Primary School will do all we reasonably can to limit children's exposure to online harms through school provided devices and networks and in line with the requirements of the Prevent Duty and KCSIE 2023, we will ensure that appropriate filtering and monitoring systems are in place.

- Emerging technologies will be examined for educational benefit and the senior management team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- The school will ensure that appropriate filtering systems are in place to prevent staff and pupils from accessing unsuitable or illegal content. We use Broadband 4 Web Filtering, an Internet Watch Foundation approved web filtering which blocks inappropriate online content.
- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- The school will audit technology use to establish if the Online Safety Policy is adequate and that the implementation of the policy is appropriate.
- Methods to identify, assess and minimise online risks will be reviewed regularly by the school's senior management team.
- Filtering decisions, internet access and device use by pupils and staff will be reviewed regularly by the school's Senior Management in conjunction with the IT Support Team.

All members of our school community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of our community. This is outlined in the acceptable usage agreements.

3.3 Appropriate and safe classroom use of the internet and associated devices (children)

- The school's internet access is designed to enhance and extend education.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will use age and ability appropriate tools to search the Internet for content. The IT support team in conjunction with the Senior Management Team provide guidance for staff on current recommendations.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability:
    - At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration with occasional directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
    - At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- All school owned devices, including any smart technology will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measures in place. These include:
    - Filtering on all school owned desktops, laptops and centrally managed Ipads.
    - Ipads for pupil use are centrally managed using Broadband 4 approved Mobile Device Management software.
    - Pupils' use of school owned devices will always take place under the direction and supervision of the class teacher or other responsible adult.
    - Network and Internet use will be monitored and any suspicious internet searches will be reported by Broadband 4 to the Senior Management Team.

Any concerns will be reported to and followed up by the Designated Safeguarding Lead.

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum.

3.4 Managing Internet Access (adults)

• We will maintain a written record of users who are granted access to our devices and systems.

• All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

3.5 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education.
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- The school will post information about safeguarding, including online safety on the school website in a specific online safety section.
- The administrator account for our website will be secured with an appropriately strong password.

3.6 Publishing images and videos online

- The school will ensure that all images are used in accordance with the school's Photographic Image Use Policy. This should be read in conjunction with this policy.
- In line with the schools photographic images policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

3.7 Managing email

- Pupils may only use school/setting provided email accounts for educational purposes as directed by staff. Emails can only be sent within the school domain. Whole –class or group email addresses may be used for communication outside of the school.
- All members of staff are provided with a specific school/setting email address to use for any official communication.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any personal chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods.
- Members of the school community must immediately tell Jill Talbot, Headteacher and Designated Safeguarding Lead (or her deputy) if they receive offensive communication and this will be recorded in the school online safety incident log.
- Sensitive or personal information will only be shared via email in accordance with data protection legislation.
- Email sent to external organisations should be written carefully in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

3.8 Official videoconferencing and webcam use

- All videoconferencing equipment in the classroom will be switched off when not in use and where appropriate, not set to auto answer.
- Equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses will not be made available to other sites.
- Staff will ensure that external videoconference are suitably risk assessed and that accounts and systems used to access events are appropriately safe and secure.
- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

Users

- All videoconferencing activities will be managed and supervised by a teacher or authorised member of staff, and will be appropriate for the pupils' age and ability.
- All videoconferencing activities must only take place after prior approval from the senior management team.
- Parents and carers consent will be obtained prior to children taking part in videoconferences as outlined in the digital images policy.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.

Content

- When recording a videoconference lesson, written permission will be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material will be stored securely.
- If third party materials are to be included, the school will check that recording is acceptable to avoid infringing the third party intellectual property rights.
- The school will establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site the school will check that they are delivering material that is appropriate for the class.

3.9 Filtering and Monitoring

3.9.1 Filtering Decision Making

- Godinton Primary School ensures that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The Governors and Senior Management Team are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

3.9.2 Filtering

• We use Broadband 4 filtering system which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
• The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
• We work to ensure that our filtering policy is continually reviewed.
• If children discover unsuitable sites, they are taught to switch off the screen. The member of staff will report the concern (including the URL of the site if possible) to the DSL and to Towers IT support. The breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child. Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

3.9.3 Monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices.
- Adults supervise and monitor the children's internet access in school.
- If a concern is identified via monitoring approaches we will complete a report of the incident on the CPOMS system and the DSL will be alerted to these.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

3.10 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).
- Full information regarding the schools approach to data protection and information governance can be found in the school's GDPR Policy.

3.11 Security and Management of Information Systems

- The security of the school information systems and users will be reviewed regularly.

- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be password protected and/or encrypted, or accessed via appropriate secure remote access systems.
- Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The IT support Team will review system capacity regularly.
- The appropriate use of user logins to access the school network will be enforced for all but the youngest users.
- All users will be expected to log off or lock their screens/devices if systems are unattended.
- The school will log and record internet use on all school owned devices using Light Speed filtering policies. A weekly log of all suspicious searches will be received from Schools Broadband and monitored by Towers IT support and the Senior Management Team. Any concerns will be reported to the Designated Safeguarding Lead.

3.11.1 Password Policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- From year 4 upwards, all children are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password. private. In Year 1, 2 and 3 passwords are generic but access is limited within our setting.
- We require all users to:
  - Use strong passwords for access into our system.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

3.12 Management of Applications (apps) used to Record Children's Progress

In the Early Years Foundation Stage we use Tapestry to track children's progress and share appropriate information with parents and carers.

The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard children's data:

- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

SECTION FOUR: SOCIAL MEDIA

4.1. Expectations of Social Media Use by all members of the school community

- Expectations regarding safe and responsible use of social media will apply to all members of Godinton Primary School (children, staff, parents, Governors, visitors etc) and exist in order to safeguard both the school and the wider community, on and offline.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms, instant messenger and other online communication services.
- Godinton Primary School believes that everyone should be treated with kindness, respect and dignity. Even though online spaces may differ in many ways, the same standards of behaviour are expected online as offline and all members of the Godinton Primary School community are expected to engage in social media in a positive and responsible manner at all times.
- All members of the school community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others.
- The use of social networking applications during school hours for personal use is not permitted using school devices. Staff may access personal social networking apps during breaks. Inappropriate or excessive use of social media during setting

hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.

- Inappropriate use of social media during school hours or whilst using school devices may result in removal of internet access and/or disciplinary action.
- Concerns regarding the online conduct of any member of Godinton Primary School community on social media will be taken seriously and should be reported to the school's Senior Management Team and will be managed in accordance with existing school policies such as anti-bullying, allegations against staff, behaviour, safeguarding/child protection and staff code of conduct. The school's whistleblowing policy should be followed.
- Information about safe and responsible use of social media will be communicated clearly and regularly to all members of the school community.
- Any breaches of school policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with the relevant school policies, such as anti-bullying, allegations against staff, behaviour, staff code of conduct and safeguarding/child protection.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our staff code of conduct policy and acceptable use of technology policy. These are shared at induction. Advice will be provided and updated via staff training and additional guidance and resources will be shared with staff as required on a regular basis.

4.1.1 Reputation

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

- Setting the privacy levels of their personal sites.
- Being aware of the implication of using location sharing services.
- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Using strong passwords and keeping passwords safe and confidential

- Ensuring staff do not represent their personal views as that of the Godinton Primary School.

Members of staff are encouraged not to identify themselves as employees of Godinton Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.

All staff are expected to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional reputation and legal framework. All members of staff are encouraged to carefully consider the information, including text and images, they share and post on social media.

Information and content that staff members have access to as part of their employment, including photos and personal information about children and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the Leadership Team immediately if they consider that an content shared on social media sites conflicts with their role

4.2 Official use of social media

- Official use of social media sites by Godinton Primary School only take s place with clear educational or community engagement objectives (e.g. increasing parental engagement) and with specific intended outcomes and once the use has been formally risk assessed and approved by the Headteacher prior to use.
- Godinton Primary School's official social media channels are:
  - *https://www.makewav.es/godinton/*
  - *https://www.youtube.com/channel/UCCVkuu4geJHE@9YmCWHc2fg*
  - *https://scratch.mit.edu/search/projects?@=godinton*
- Official social media sites are suitably protected and, where possible run from our school website. Official social media channels have been set up as distinct and dedicated accounts for official education or engagement purposes only. Staff use setting provided email addresses to register for and manage official social media channels. Leadership staff have access to account information and login details for social media channels.
- Official social media use will be conducted in line with existing policies, including but not limited to anti-bullying, photographic images, data protection / GDPR, confidentiality and child protection.
- All communication on official social media platforms by staff on behalf of the school will be clear, transparent and open to scrutiny. Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.

- Parents and carers and children will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
- Parents and carers will be informed of any official social media use with children/pupils/students; any official social media activity involving children/pupils/students will be moderated if possible and written parental consent will be obtained as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.
- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts where possible, to avoid blurring professional boundaries.
- If members of staff are managing and/or participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Read and understand our Acceptable Use Policy.
  - Where they are running official accounts, sign our social media Acceptable Use Policy. If implemented.
  - Be aware they are an ambassador for the school.
  - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection and equalities laws.
  - Follow our photographic images policy at all times, for example ensuring that appropriate consent has been given before sharing images.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any private or direct messaging with current or past children or their family members.
  - Inform the Headteacher and the DSL (or deputy) of any concerns, such as criticism, inappropriate content or contact from children.

4.3 Children's Use of Social Media

- Children are not permitted to use any social media for personal use during school hours.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents are responsible for this behaviour; however, some online incidents may affect our culture and pose a risk to children and young people's health and well-being. Where online behaviour

online poses a threat or causes harm to another child, could have repercussions for the orderly running of the school when the child is identifiable as a member of the school, or if the behaviour could adversely affect the reputation of the school, action will be taken in line with our behaviour and child protection/online safety policies.

- Godinton Primary School will empower our children to acquire the knowledge needed to use social media in a safe, considered and respectful way, and develop their resilience so they can manage and respond to online risks. Safe and appropriate use of social media will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies for example, RSE. PSHE and Computing.
- We are aware that many popular social media sites are not permitted for use by children under the age of 13, or in some cases higher. As such, we will not create accounts for children under the required age as outlined in the services terms and conditions.
- Safe and responsible use of age appropriate social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy.
- Children will be advised to consider the risks of sharing personal details of any kind on social media sites that may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- Children will be advised to only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private. They will be supported in learning how to block and report unwanted communications.
- Children will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Children will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Children will be taught how to report concerns on social media.
- Any concerns regarding children's use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- Concerns will be raised with their parents/carers, particularly when concerning any underage use of social media sites. The DSL or deputy will respond to social media concerns involving safeguarding or child protection risks in line with our safeguarding policy.
- Sanctions and / or pastoral welfare support will be implemented and offered to children as appropriate, in line with our child protection and behaviour policy. Civil or legal action may be taken if necessary.

4.4 Communicating with learners and parents and carers

- Staff will not use any personal social media accounts to contact children or their family members.
- All members of staff are advised not to communicate with or add any current or past children or their family members as 'friends' on any personal social media accounts.
- Any pre-existing relationships or situations, which mean staff cannot comply with this requirement, will be discussed with the DSL and the Headteacher.
- Staff should email parents using the year group email accounts or ask parents to contact them via the school office. They may use their personal school email account should they wish.
- Any communication from children and parents received on personal social media accounts will be reported to the DSL.

SECTION FIVE: USE OF PERSONAL DEVICES AND MOBILE PHONES

5.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among children, young people and adults will require all members Godinton Primary School to take steps to ensure that mobile phones and personal devices are used responsibly.
- The use of mobile phones and other personal devices by young people and adults will be decided by the school and covered in appropriate policies including the school Acceptable Use Policy
- Godinton Primary School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers but requires that such technologies need to be used safely and appropriately within school.

5.2 Expectations for safe use of personal devices and mobile phones

- Electronic devices of all kinds that are brought in to school are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- All members of the Godinton Primary School community are advised to:
  - take steps to protect their mobile phones or personal devices from loss, theft or damage;
  - use passwords/PIN numbers to ensure that unauthorised access, calls or actions cannot be made on their phones or devices.

- Mobile phones and personal devices are not permitted to be used in specific areas on site, including toilets and when staff are in the classrooms or others areas of the school site in the presence of children (unless specific permission has been sought). When offsite, mobile phones and personal devices are not to be used in public toilets or changing rooms.
- The sending of abusive or inappropriate messages or content, including via personal smart devices and mobile phones is forbidden by any member of the community; any breaches will be dealt with in line with our anti-bullying, behaviour and child protection policies or staff disciplinary policies.
- All members of the Godinton Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or illegal, or which would otherwise contravene our behaviour or child protection policies.

5.3 School provided mobile phones and devices

- Work mobile phones are provided to the Family Liaison Officer in order for her to make contact with parents and to the Site Manager in order to deal with queries related to the premises, including out of hours. Teaching staff, and some other support staff are provided with a school laptop. These devices can be used off site.
- School mobile phones and devices will be suitably protected via a password and/or PIN and must only be accessed or used by members of staff.
- School mobile phones and devices will always be used in accordance with our staff code of conduct/behaviour policy, acceptable use of technology policy and other relevant policies.
- The school has a series of laptops which can be borrowed by children in order to assist with remote learning. When these are issued, an AUP is signed and the expectation is that the device will be used in accordance with this policy.
- Where staff and/or children/pupils/students are using school/setting provided mobile phones and/or devices, they will be informed prior to use via our Acceptable Use Policy (AUP) that activity may be monitored for safeguarding reasons and to ensure policy compliance.

5.4 Staff use of mobile and smart technology

- Members of staff will ensure that use of any mobile and smart technology, including personal phones and mobile devices, will take place in accordance with the law, as well as relevant school/setting policy and procedures, such as confidentiality, child

protection, data security staff behaviour/code of conduct and Acceptable Use Policies.

- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place (e.g. locked drawer or cupboard) during lesson time.
  - Keep personal mobile phones and devices switched off or set to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods unless permission has been given by the Headteacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via personal mobile phones and devices is compatible with their professional role and our behaviour expectations.

- Members of staff are not permitted to use their own personal phones or devices for contacting parents, unless in emergency situations as agreed by the Headteacher. Members of staff are not permitted to use their own personal phones or devices to contact children

- Any pre-existing relationships or circumstance, which could compromise staff's ability to comply with this, will be discussed with the Headteacher / DSL.

- Staff will only use school/setting provided equipment (not personal devices):
  - to take photos or videos of children in line with our photographic images policy.
  - to work directly with children during lessons/educational activities.
  - to communicate with parents (unless in an emergency situation as agreed above).

- Where remote learning activities take place, staff will use school provided equipment. If this is not available, staff will only use personal devices with prior approval from the Headteacher, following a formal risk assessment. Staff will follow clear guidance outlined in the Acceptable Use Policy.

- If a member of staff breaches our policy, action will be taken in line with our staff behaviour policy/code of conduct and allegations policy.

- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence using a personal device or mobile phone, the police will be contacted and the LADO (Local Authority Designated Officer) will be informed in line with our allegations policy.

5.5 Pupils use of mobile and smart technology

Children will be educated regarding the safe and appropriate use of mobile and smart technology, including mobile phones and personal devices, and will be made aware of behaviour expectations and consequences for policy breaches.

Safe and appropriate use of mobile and smart technology will be taught to children as part of an embedded and progressive safeguarding education approach using age-appropriate sites and resources. Further information is contained within our child protection and relevant specific curriculum policies for example, PSHE, RSE and Computing.

Pupils are not permitted to have mobile phones on their person at any time during the school day. Where a child brings a mobile phone to school to use in an emergency situation on their way to and from school, it must be switched off and handed into the school office at the start of the day. The school will not be responsible for any loss or damage to a child's phone which has been brought onto school premises. Devices are handed in to the school office at the owner's risk.

Staff may confiscate a child's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting). Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the school day. If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Children are permitted to wear smart watches to school providing that they are set to 'school mode' and therefore are not connected to the internet. This arrangement is made in conjunction with parents.

Where children/pupils/students' mobile phones or personal devices are used when learning at home, this will be in accordance with our Acceptable Use Policy and/or Remote Learning AUP.

5.6 Visitors use of mobile and smart technology

Parents/carers and visitors, including volunteers and contractors, are expected to ensure that:

Mobile phones and personal devices are not used in specific areas on site, including toilets and when in the presence of children in classrooms or areas of the school.

Appropriate signage and information are in place to inform visitors of our expectations for safe and appropriate use of personal devices and mobile phones.

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use of technology policy and other associated policies, including child protection.

If visitors require access to mobile and smart technology, for example when working with children as part of multi-agency activity, this will be discussed with the Headteacher prior to use being permitted. Any arrangements regarding agreed visitor access to mobile/smart technology will be documented and recorded by the school/setting. This may include undertaking appropriate risk assessments if necessary.

Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL / Headteacher of any breaches of our policy.

SECTION SIX: POLICY DECISIONS

6.1. Internet use throughout the wider school community

- The school will take advice from the Kent Education Safety Safeguarding Service (accessed through The Education People) to establish a common approach to online safety.
- The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site

6.2 Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff, pupils and visitors will read and sign the School Acceptable Use Policy before using any school IT resources.
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the pupil(s).

SECTION SEVEN: RESPONDING TO ONLINE INCIDENTS AND CONCERNS

All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyberbullying, illegal content etc.).

- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be recorded.
- The Designated Safeguarding Lead (DSL) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Kent Safeguarding Children Multi Agency Partnership (KSCMP) thresholds and procedures.
- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Complaints about online bullying will be dealt with under the School's anti-bullying policy and procedure
- Any complaint about staff misuse will be referred to the Headteacher
- Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Pupils, parents and staff will be informed of the schools complaints procedure.
- Staff will be informed of the complaints and whistleblowing procedure.
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online that cause harm, distress or offence to any other members of the school community.
- The school will manage online safety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguarding Team or Kent Police via 999 if there is immediate danger or risk of harm.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Kent Police.
- If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.

- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Kent.
- Parents and children will need to work in partnership with the school to resolve issues.

SECTION EIGHT: PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

Further, more detailed information can be found in the school's Child Protection (Safeguarding) Policy.

8.1 Child on Child Sexual Violence and Sexual Harassment

When responding to concerns relating to child on child sexual violence or harassment, our school will follow the guidance outlined in Part Five of KCSIE 2022.

Guidance is provided in Childnet's online sexual harassment guidance:

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

Further information about child on child sexual violence and sexual harassment can be found in the school's Child Protection Policy.

Godinton Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include;

- Non-consensual sharing of sexual images and videos
- Sexualised online bullying
- Online coercion and threats
- 'Upskirting', which typically involves taking a picture under a person's clothing without them knowing, with the intention of obtaining sexual gratification, or causing the victim humiliation, distress or alarm. It is a criminal offence.
- Unwanted sexual comments and messages on social media
- Online sexual exploitation

We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of any concerns relating to online sexual violence and sexual harassment, we will:

- Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
- If content is contained on learners personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice. Further information on this can be found in the school's Behaviour and Discipline Policy.

- Provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make referrals to partner agencies, such as Children's Social Services and/or the police.
- If the concern involves children and young people at a different educational setting, the DSL will work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL (or deputy) will discuss this with the police first to ensure that investigations are not compromised.
- We will review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.
- Godinton Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Godinton Primary School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Godinton Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment by implementing a range of age and ability appropriate educational methods as part of our curriculum. We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between learners.

8.2 Nude and/or Semi-Nude Image Sharing by Children

The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of eighteen (this used to be referred to as sexting). Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".

The UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance outlines how schools and colleges should respond to all incidents of consensual and non-consensual image sharing; it should be read and understood by all DSLs working with all age groups.

Our school recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting")

can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, forward, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already inadvertently viewed imagery , this will be immediately reported to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

DSLs will respond to concerns in line with the non-statutory UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people' and the local KSCMP guidance. When made aware of a concern involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos:

The DSL will hold an initial review meeting to explore the context and ensure appropriate and proportionate safeguarding action is taken in the best interests of any child involved. This may mean speaking with relevant staff and the children involved as appropriate.

Parents and carers will be informed at an early stage and be involved in the process to best support children, unless there is good reason to believe that involving them would put a child at risk of harm.

All decisions and action taken will be recorded in line with our child protection procedures.

A referral will be made to ICS and/or the police immediately if:

- the incident involves an adult (over 18).
- there is reason to believe that a child has been coerced, blackmailed, or groomed, or there are concerns about their capacity to consent, for example, age of the child or they have special educational needs.
- the image/videos involve sexual acts and a child under the age of 13, depict sexual acts which are unusual for the child's developmental stage, or are violent.
- a child is at immediate risk of harm owing to the sharing of nudes and semi-nudes.

The DSL may choose to involve other agencies at any time if further information/concerns are disclosed at a later date.

If DSLs are unsure how to proceed, advice will be sought from the Education Safeguarding Service.

8.3 Online Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

- Godinton Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Godinton Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. This is available on our website and children will be educated about when they need to use it.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Kent Safguarding Children Multi-Agency Partnership procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Services (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented;
- leadership team will review and update any management procedures, where necessary
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or Kent Police.

- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSET) by the DSL.
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

8.4 Indecent Images of Children (IIOC)

- Godinton Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If it is unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Kent Police and/or the Education Safeguarding Team.
- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Kent Safguarding Children Multi-Agency Partnership procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Kent police or the LADO.
- If made aware that a member of staff or a child has been inadvertently exposed to indecent images of children, we will:
- Ensure that the DSL is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

- If made aware that indecent images of children have been found on the setting provided devices, we will:
- Ensure that the DSL is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk . Ensure that any copies that exist of the image, for example in emails, are deleted. Inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.

• If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy. Quarantine any devices until police advice has been sought.

8.5 Cyberbullying

• Cyberbullying, along with all other forms of bullying, will not be tolerated at Godinton Primary School.

• Full details of how we will respond to cyberbullying are set out in our anti-bullying policy

7.6 Online Hate

• Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Godinton Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.

• All members of the community will be advised to report online hate in accordance with relevant policies and procedures.

• The Police will be contacted if a criminal offence is suspected.

• If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice through the Education Safeguarding Team and/or Kent Police.

Further information can be found in the school's Child Protection Policy.

8.6 Online Radicalisation and Extremism

• We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

• If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our child protection policy.

• If we are concerned that a member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

Further information can be found in the school's Child Protection Policy.

8.7 Online Safety During Remote Learning

Specific guidance for DSLs and SMT regarding remote learning is available at DfE: Safeguarding and remote education during coronavirus (COVID-19) and The Education People: Remote Learning Guidance for SMT.

Godinton Primary School will ensure any remote sharing of information, communication and use of online learning tools and systems will be in line with privacy and data protection requirements and local guidance.

All communication with children and parents/carers will take place using school provided or approved communication channels; for example, school provided email accounts and phone numbers and/or agreed systems e.g. Microsoft 365, Purple Mash and Tapestry.

Staff and children will engage with remote teaching and learning in line with existing behaviour principles as set out in our school behaviour policy, Staff Code of Conduct and Acceptable Use Policies.

Staff and children will be encouraged to report issues experienced at home and concerns will be responded to in line with our child protection and other relevant policies.

When delivering remote learning, staff will follow the guidance on Remote Learning which is outlined in the Acceptable Usage Policy.

Parents/carers will be made aware of what their children are being asked to do online, including the sites they will be asked to access. Godinton Primary School will continue to be clear who from the school/college (if anyone) their child is going to be interacting with online.

Parents/carers will be encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented at home. Guidance is provided for parents.

SECTION NINE– EQUALITY STATEMENT (Refer also to specific policies for equal opportunities and racial equality)

At Godinton Primary School, we are committed to ensuring equality of opportunity for all members of our school community irrespective of race, religion or belief, gender, gender reassignment, disability, sexual orientation, age, pregnancy or maternity, marriage and civil partnership or socio-economic background. We are determined to develop a culture of inclusion and diversity in which all those connected to the school feel proud of their identity and ability to participate fully in school life.

We tackle discrimination through the positive promotion of equality by challenging stereotypes and by creating an environment that champions respect for all. At Godinton Primary School, we believe that diversity is a strength that should be respected and celebrated by all those who learn, teach and visit us.

All school policies have an explicit aim of promoting equality and will be reviewed in terms of their contribution and effectiveness in achieving this aim.

SECTION TEN – CHILDREN IN CARE

As for all our pupils, Godinton Primary School is committed to helping every Child in Care (CIC) to achieve the highest standards they can. To this end staff will ensure that in delivering the curriculum they set suitable learning challenges of CIC, respond to the diverse learning needs of CIC, and help to overcome the potential barriers to learning and assessment for CIC. The relevant subject coordinators will support staff in doing this within this subject.

SECTION ELEVEN – POLICY REVIEW

- Technology in this area evolves and changes rapidly. Godinton Primary School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher (Online Safety Lead and DSL) will be informed of online safety concerns, as appropriate.
- Any issues identified via monitoring will be incorporated into our action planning
- Online safety is included in the annual safeguarding review for Governors and as part of the safeguarding section of the Headteacher's report to the Full Governing Body.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.

APPENDIX ONE Useful Links for Educational Settings

All members of staff in Godinton Primary School are made aware of local support available. This information can be located on the safeguarding board in the school staff room.

If a child may be at risk of imminent harm, you should call the

Integrated Front Door on 03000 411111 or the Police on 999

Contact details for Area Safeguarding Adviser (Education Safeguarding Team)

Area Safeguarding Advisor (Education) South Kent Safeguarding Advisor: Gemma Willson (Monday/Tuesday) Claire Ledger (Wednesday/Thursday/Friday)

Office: Ashford – 03000 423 154

Contact details for Online Safety (Education Safeguarding Team)

03000 423164

onlinesafety@theeducationpeople.org (non-urgent issues only)

Contact details for the LADO

Telephone: 03000 410888

Email: kentchildrenslado@kent.gov.uk

Integrated Front Door: 03000 411111 (outside office hours 03000 419191)

Early Help Contacts can be found on www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Kent Police

101 (or 999 if there is an immediate risk of harm)

Kent Safeguarding Children Multi-Agency Partnership (KSCMP)

kscmp@kent.gov.uk

www.kscmp.org.uk

03000 421126

Adult Safeguarding

Adult Social Care via 03000 41 61 61 (text relay 18001 03000 41 61 61) or email social.services@kent.gov.uk

Central Team

Head of Service: Claire Ray – 03000 423 169

Training and Development Manager: Rebecca Avery – 03000 423 168

Senior Safeguarding Advisor: Robin Brivio – 03000 423 169

Online Safety: Ashley Assiter, Online Safety Development Officer (Monday/Tuesday/Wednesday) – 03000 423 164

- **Guidance for Educational Settings:**

www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding

www.theeducationpeople.org/blog/?tags=Online+Safety&page=1

Other:

- EiS – ICT Support for Schools and Kent Schools Broadband Service Desk: www.eisit.uk

National Links and Resources for Settings, Learners and Parents/carers

CEOP:

www.thinkuknow.co.uk

www.ceop.police.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

UK Council for Internet Safety (UKCIS):

www.gov.uk/government/organisations/uk-council-for-internet-safety

UK Safer Internet Centre: www.saferinternet.org.uk

Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline

Report Harmful Content: https://reportharmfulcontent.com/

360 Safe Self-Review tool for schools: www.360safe.org.uk

Childnet: www.childnet.com

Step Up Speak Up – Online Sexual Harassment Guidance:

www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-andprofessionals

Cyberbullying Guidance: www.childnet.com/resources/cyberbullying-guidance-for-schools

Internet Matters: www.internetmatters.org

Parent Zone: https://parentzone.org.uk

Parent Info: https://parentinfo.org

NSPCC: www.nspcc.org.uk/onlinesafety

ChildLine: www.childline.org.uk

Net Aware: www.net-aware.org.uk

Lucy Faithfull Foundation: www.lucyfaithfull.org

The Marie Collins Foundation: www.mariecollinsfoundation.org.uk

Action Fraud: www.actionfraud.police.uk

Get Safe Online: www.getsafeonline.org

Responding to an Online Safety Concern

APPENDIX TWO

Online Safety Incident

Contact or Conduct

This may include CEOP

Report to agencies, as appropriate and in line with child protection procedure.

Key Local Contacts

Designated Safeguarding Lead (s): Name, Role and contact info

Area Education Safeguarding Advisor: Name, contact info

Education Safeguarding Advisor (Online Safety): Rebecca Avery 03000 415797

Front Door: 03000 411111

LADO: 03000 410888

Kent Police: 101 or 999 if immediate risk of harm

Illegal Content

- **Accidental Exposure** → Report to DSL → Consult with Education Safeguarding Service → Report to Internet Watch Foundation (www.iwf.org.uk), Kent Police and/or Front Door as appropriate
- **Deliberate**
  - **Child** → Report to DSL → Consult with Education Safeguarding Service → Report to Internet Watch Foundation (www.iwf.org.uk), Kent Police and/or Front Door as appropriate
  - **Member of Staff** → Report to Headteacher (or equivalent in line with allegations policy) → Consult with LADO
    - Consult with LADO → **Possible Internal Actions**
      - Staff training
      - Disciplinary action if deliberate – contact personnel provider
      - School support e.g. counselling
      - Request support/advice from Education Safeguarding Service
    - Consult with LADO → If criminal or child protection investigation required → Report to Internet Watch Foundation (www.iwf.org.uk), Kent Police and/or Front Door as appropriate

Unsure → Consult with Education Safeguarding Service

Inappropriate Conduct or Content

- **Conduct**
  - **Member of Staff** → Report to Headteacher (or equivalent in line with allegations policy) → Consult with LADO → **Possible Internal Actions**
    - Staff training
    - Disciplinary action if deliberate – contact personnel provider
    - School support e.g. counselling
    - Request support/advice from Education Safeguarding Service
  - **Child** → Report to DSL → **Possible Internal Actions**
    - Sanctions (if deliberate)
    - PSHE/citizenship
    - Restorative justice
    - Anti-bullying
    - Parental work
    - School support e.g. counselling, peer mentoring
    - Request support/advice from Education Safeguarding Service
- **Content** → Report to Internet and/or Filtering Service Provider

Record incident and action taken. Review policies and procedures and implement changes