Foreland Fields School
Online Safety Policy

Governing Body Approval and Categories

Date of Last Review / Scrutiny	29th September 2026
Date (Month / Year) of Next Review /Scrutiny	29th September 2027
Date Policy was Ratified	7th October 2026
Category of the Policy	Safeguarding
Named Lead for Writing the Policy	Headteacher/DSL
Named Governor for Scrutiny	Governor with Responsibility for Safeguarding – Nicola Elson
Approval Body	Full Governing Body
Display on Main Web Site	Yes
NOTE: IF THIS POLICY HAS BEEN SCRUTINISED BY A DIFFERENT LEAD GOVERNOR OR BEEN RATIFIED BY A DIFFERENT GOVERNING TEAM PLEASE STATE WHICH TEAM	
Signed – Chair of Governors	Date 7-10-26

United Nations Convention on the Rights of the Child

Foreland Fields School is a Rights Respecting School thereby this policy ensures that the following rights are acknowledged:

Article 3 (best interests of the child) The best interests of the child must be a top priority in all decisions and actions that affect children.

Article 17 (access to information from the media) Every child has the right to reliable information from a variety of sources, and governments should encourage the media to provide information that children can understand. Governments must help protect children from materials that could harm them.

Article 19 (protection from violence, abuse and neglect). Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and bad treatment by their parents or anyone else who looks after them.

Article 28 (right to education). Every child has the right to an education. Primary education must be free and different forms of secondary education must be available to every child. Discipline in schools must respect children's dignity and their rights.

Online Safety Policy

[Including reference to Mobile and Smart Technology and Social media]

Foreland Fields School

September 2026

Contents

1. Policy Aims 6
2. Policy Scope 7
    2.2 Links with other policies and practices 7
3. Monitoring and review and responding to policy breaches 7
4. Roles and Responsibilities 8
    4.1 The leadership and management team 8
    4.2 The Designated Safeguarding Lead 8
    4.3 Members of staff 9
    4.4 Staff who manage the technical environment 10
    4.5 Pupils 10
    4.6 Parents 10
5. Education and Engagement Approaches 11
    5.1 Education and engagement with pupils 11
    5.2 Vulnerable pupils 12
    5.3 Training and engagement with staff 13
    5.4 Awareness and engagement with parents/carers 13
6. Reducing Online Risks 14
7. Safer Use of Technology 14
    7.1 Classroom Use 13
    7.2 Managing Internet Access 15
    7.3 Filtering and Monitoring 16
    7.4 Managing Personal Data Online 17
    7.5 Security and Management of Information Systems 17
    7.6 Managing the Safety of the Website 18
    7.7 Publishing Images and Videos Online 18
    7.7.1 SeeSaw, ClassDojo and Evidence for Learning 19
    7.8 Managing Email 20
    7.9 Educational use of Video conferencing and/or Webcams 21
    7.10 Management of Learning Platforms – SeeSaw 23

    7.11 Management of Applications (apps) used to Record Pupil's Progress
    7.12 Remote Working; Pulse Secure
    7.13 Use of IRIS to support Staff Development. 24
    7.14 Use of Music streaming Apps and Voice control technology 25
    7.15 Use of MyConcern to record safeguarding concerns 25
    7.16 Use of IRS adapt to record accidents, behaviour incidents, errors in the administration of medication and medical incidents. 25
    7.15 Generative Artificial Intelligence

8. Social Media 26
8.1 Expectations 26
8.2 Staff Personal Use of Social Media 26
8.3 Pupil's Personal Use of Social Media 28
8.4 Official Use of Social Media 29
9. Use of Mobile and Smart Technology 30
9.1 Expectations 30
9.2 Staff Use of Mobile and Smart Technology 31
9.3 Pupil's Use of Mobile and Smart Technology 32
9.4 Visitors' Use of Mobile and Smart Technology 33
9.5 Officially provided Mobile and Smart Technology 35

10. Responding to Online Safety Incidents and Concerns 34
10.1 Concerns about Learner Welfare 34
10.2 Concerns about staff online behaviour/welfare 35
10.3 Concerns about parent/carer online behaviour and/or welfare 35
11. Procedures for Responding to Specific Online Incidents or Concerns 35
11.1 Online Sexual Violence and Sexual Harassment between Children 34
11.2 Nude and/or Semi-Nude Image Sharing by Children 37
11.3 Online Child Sexual Abuse and Exploitation 38
11.4 Indecent Images of Children (IIOC) 39
11.5 Cyberbullying and Cybercrime 40
11.6 Online Hate 40
11.7 Online Radicalisation and Extremism 41
12. Responding to an Online Incident. 44
13. Links and Contacts. 45

Foreland Fields School

Online Safety Policy

Key Details

Designated Safeguarding Lead - Responsibility for Online Safety (s):

Adrian Mount, Headteacher

Named Governor with Lead Responsibility: Nicola Elson

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

Foreland Fields School Online Safety Policy

1. Policy Aims

- This online safety policy has been written by Foreland Fields School involving staff, pupils, Governors and parents/carers, building on Kent County Councils LADO, Education Safeguarding Advisory Service online safety, mobile and smart technology and social media policy templates, with specialist advice and input as required.
- It should be noted that from 29th June 2026 the school, in response to updated guidance has a separate Mobile Phone and Smart Technology Policy. This policy contains reference to mobile and smart technology, but staff and parents/carers should refer to the Mobile Phone and Smart Technology Policy for guidance in this area.
- It takes into account the Department for Education (DfE) statutory guidance 'Keeping Children Safe in Education' (KCSIE), Early Years and Foundation Stage (EYFS), 'Working Together to Safeguard Children' (WTSC), the DfE non-statutory guidance 'Behaviour in Schools Advice for headteachers and school staff', 'Searching, screening and confiscation at school' , 'mobile phones in schools June 2026 https://www.gov.uk/government/publications/mobile-phones-in-schools/mobile-phones-in-schools#implementing-a-policy-on-prohibiting-the-use-of-mobile-phones and the local Kent Safeguarding Children Multi-agency Partnership (KSCMP) procedures.
- The purpose of this policy is to safeguard and promote the welfare of all members of the Foreland Fields community when using mobile devices and smart technology.
  a. Foreland Fields recognises that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm when online and using mobile and smart technology.
  b. As outlined in our Child Protection Policy, the Designated Safeguarding Lead (DSL), Adrian Mount, Headteacher is recognised as having overall responsibility for online safety.
  c. Identify approaches to educate and raise awareness of online, mobile device, smart technology and social media safety throughout the community.
  d. Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
  e. Identify clear procedures to use when responding to online safety concerns.

- Foreland Fields 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 content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
  - Contact: being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
  - Conduct: personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (e.g. consensual and non-consensual

sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
    - Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

- Foreland Fields School recognises that technology, and the risks and harms related to it, evolve and change rapidly. The school will carry out an annual review of our approaches to online safety, supported by an annual risk assessment which considers and reflects the risks our children face.

- The Headteacher will be informed of online safety concerns by the designated teacher, as appropriate. The named governor for safeguarding will report on online safety practice and incidents, including outcomes, on a regular basis to the wider Governing Body.

2. Policy Scope

- Foreland Fields School believes that online, mobile device, smart technology and social media safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Foreland Fields School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Foreland Fields School believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all access to and use of all mobile and smart technology on site; 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.
- This policy applies to pupils, 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).

2.2 Links with other policies and practices

- This policy links with several other policies, practices and action plans including:
    - Safeguarding policy
    - Acceptable Use policies including Visitor and Wi-Fi AUPs
    - Camera and image use policy
    - Confidentiality policy
    - Anti-Bullying Policy
    - GDPR and data security
    - Sex & Relationship Education Policy
    - Staff Behaviour Policy
    - Risk Assessments (e.g. school trips, use of technology)
    - Managing Allegations Against Staff Members Policy
    - Staff Behaviour Policy (Staff Code of Conduct)
    - Safer Recruitment Policy
    - Whistleblowing Policy

3. Monitoring and Review and Responding to Policy Breaches

- Technology in this area evolves and changes rapidly. Foreland Fields School will review this policy at least annually (as a minimum).
    - The policy will also be revised following any national or local policy requirements; any child protection concerns or any changes to the technical infrastructure
- All staff (including temporary staff and volunteers) will be provided with a copy of this policy. This will be sent to staff via MyConcern and can also be found on KLZ SharePoint.
- 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 will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Full information about the appropriate filtering and monitoring systems in place are detailed in our Child Protection Policy and in section 7.3 of this policy document. Any issues identified as part of the implementation of our monitoring approaches will be incorporated into our action.
- Any issues identified via monitoring will be incorporated into our action planning.

Responding to policy breaches

- All members of the community are informed of the need to report policy breaches or concerns in line with existing school policies and procedures.
- After any investigations are completed, leadership staff will debrief, identify lessons learnt and implement any policy or curriculum changes, as required.
- We require staff, parents/carers and pupils to work in partnership with us to resolve issues.
- All members of the community will respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher will seek advice from Kent County Council or other agencies, as appropriate, in accordance with our child protection policy.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) (Adrian Mount, Headteacher) has lead responsibility for online safety.
- Foreland Fields School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The leadership and management team will:

- Create a whole setting culture that incorporates online safety throughout all elements of life at Foreland Fields School.
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks. The school currently uses Netsweeper, which is provided through Medway Grid for Learning for its education broadband connectivity.
- Ensure that online safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

4.2 The Designated Safeguarding Lead will ensure that:

- They act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Liaise with other members of staff, such as Class based staff, the wider SLT, the FLO and the network manager on matters of online safety.
- Ensure that locally established procedures as put in place by the three safeguarding partners as part of the Kent Safeguarding Children Multi-Agency Partnership procedures (KSCMP), including referrals, are followed as necessary.
- Ensure online safety is recognised as part of the settings safeguarding responsibilities and that a coordinated approach is implemented. Ensure all members of staff receive regular, up-to-date and appropriate and wide-ranging online safety training, to include links to safeguarding and radicalisation / extremism.
- Access 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 pupils safe online.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and child protection training.
- Access regular and appropriate training and support to ensure they recognise the additional risks that pupil's with SEN and disabilities (SEND) face online. These might include:

- Assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's condition without further exploration.
- These children being more prone to peer group isolation or bullying (including prejudice-based bullying) than other children.
- The potential for children with SEND or certain medical conditions being disproportionally impacted by behaviours such as bullying, without outwardly showing any signs.
- Communication barriers and difficulties in managing or reporting these challenges.
- Cognitive understanding – being unable to understand the difference between fact and fiction in online content and then repeating the content/behaviours in schools or colleges or the consequences of doing so.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Monitor Online Safety on a weekly basis via having Online Safety as a standing item in weekly safeguarding meetings.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly three times a year with the governor with a lead responsibility for online safety. Additionally (Adrian Mount), the entire Online safety team, which comprises the DSL, Deputy DSL PSHE and Computing leads, the Governor with responsibility for Online Safety, a parent, the school network manager and teaching staff also meet three times a year.

4.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.

- 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.
- Take personal responsibility for professional development in this area.
- Reassure children who report concerns that they are being taken seriously and that they will be supported and kept safe.

4.4 It is the responsibility of staff managing the technical environment to:

- 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 *(*see section 7*)* 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 leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- 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.

4.5 It is the responsibility of pupils (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Confidently report abuse, knowing their concerns will be treated seriously, and knowing they can safely express their views and give feedback.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.

- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

5.1 Education and engagement with pupils

- Foreland Fields will establish and embed a whole school culture and will raise awareness and promote safe and responsible internet use amongst learners by:
    - ensuring our curriculum and whole school approach is developed in line with the UK Council for Internet Safety (UKCIS) 'Education for a Connected World Framework' and DfE 'Teaching online safety in school' guidance. These documents and guidance will be used alongside an understanding the complex needs of the pupils at the school. The implementation of 'Education for a connected world framework' is most relevant to our pupils who are studying our formal curriculum.
    - ensuring online safety is addressed appropriately (starting from pupil need, within the informal, semi-formal and formal curricula). Within the formal curriculum this will be delivered through Relationships Education, Relationships and Sex Education, Health Education, Citizenship and Computing programmes of study. Within the semi-formal curriculum, a skills-based approach, which targets the development of accessible strategies to stay safe will be utilised. For example, this will include understanding the need for supervision, recognising danger and knowing how to get support.
    - reinforcing online safety principles in other curriculum subjects as appropriate, and whenever technology or the internet is used on site.
    - implementing appropriate peer education approaches.
    - creating a safe environment in which all pupils feel comfortable to say what they feel, without fear of getting into trouble and/or being judged for talking about something which happened to them online.
    - involving the DSL (or a Deputy) as part of planning for online safety lessons or activities, so they can advise on any known safeguarding cases, and ensure support is in place for any pupils who may be impacted by the content.
    - making informed decisions to ensure that any educational resources used are appropriate for our pupils.
    - using external visitors, where appropriate, to complement and support our internal online safety education approaches.
    - rewarding positive use of technology.

- Foreland Fields School will support pupils to understand and follow our acceptable use policies in a way which suits their age and ability by:
    - displaying acceptable use posters in all rooms with internet access.
    - informing pupils that network and internet use will be monitored for safety and security purposes, and in accordance with legislation.
    - seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Foreland Fields School will ensure pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability by:
    - ensuring age appropriate education regarding safe and responsible use precedes internet access.
    - teaching pupils to evaluate what they see online and recognise techniques used for persuasion, so they can make effective judgements about if what they see is true, valid or acceptable.
    - educating them in the effective use of the internet to research, including the skills of knowledge location, retrieval and evaluation.
    - enabling them to understand what acceptable and unacceptable online behaviour looks like.
    - preparing them to identify possible online risks and 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.

5.2 Vulnerable pupils

- Foreland Fields School recognises that some pupils 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.
- Foreland Fields School educates pupils with a wide range of needs, but all have severe learning delays and communication difficulties, which means all schemes of work must be adapted to reflect these needs to ensure true accessibility.
- Foreland Fields School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. A wide range of SEN specific Online Safety resources are available on the school shared drive and these are continually updated and adapted by teaching staff who then share these resources with the rest of the staff team.
- The school recognises the vulnerability of its pupils to issues such as radicalisation, extremism and inappropriate use social media, sexting and stranger danger. As such these issues are taught, as appropriate through the curriculum and in response to specific incidents.

- Technology can be a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face and in many cases, abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online.
- When implementing an appropriate online safety policy and curriculum Foreland Fields School will seek input from specialist staff as appropriate, including the Child in Care Designated Teacher and the Network manager.

5.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Foreland Fields School will ensure that all staff receive online safety training, which, amongst other things, will include providing them with an understanding of the expectations, applicable roles and their responsibilities in relation to filtering and monitoring, as part of induction.
- Ongoing online safety training and updates for all staff will be integrated, aligned and considered as part of our overarching safeguarding and child protection training approach.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
    - Discrete Online safety training is delivered annually by the Deputy Designated Safeguarding Lead with responsibility for online safety and is based on the KCC online safety training package.
    - This will cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

5.4 Awareness and engagement with parents and carers

- Foreland Fields School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

- We will build a partnership approach to online safety with parents and carers to become aware and alert of the potential online benefits and risks for children by:
  - Having discussions regarding online safety in all EHCP reviews.
  - Offering support to parents regarding restricting access / firewalls.
  - Providing information and guidance on online safety in a variety of formats.
  - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
  - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website. Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
  - Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

- Foreland Fields School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the 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 the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom use

- Foreland Fields School uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - Games consoles and other games-based technologies
  - Digital cameras, web cams and video cameras
  - Educational communication app, ClassDojo
  - Eyegaze inclusive technology

- All school owned devices will be used in accordance with the school's AUP's (including Wi-Fi AUP) and with appropriate safety and security measures in place. All tablets are controlled and managed by MDM Lightspeed. Mobile Device Manager (MDM) solution ensures that all purchased apps are correctly licensed and all tablet settings can be adjusted, 'locked down' and/or turned off if necessary. Devices or applications that can make students vulnerable (FaceTime, Skype, the iPads camera as just a few examples) can be simply switched off from this centrally managed cloud system. User access to the internet via the mobile devices is monitored through 'Captive Portal' on Lightspeed Filtering. Captive Portal will force users to login via the Lightspeed Login page prior to internet browsing and all activity is recorded and included in the weekly 'Foreland Field Web Activity' report.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools. Search engines in place and to be utilised by the pupils within school, include Google Safe Search Kids and KidRex. Older pupils are allowed access to 'Google' but are taught to use these tools safely and responsibly. However, it must be noted, that mainstream 'Google' search results are still passing through the school's filtering system and Google Safe Search is enforced (via EIS) in the background.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability rather than by key stage. All use of online tools at Foreland Fields School is supervised. Most children will fit into one of two categories;

  i) 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.

  ii) Pupils will use age-appropriate search engines and online tools. Children will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupils' age and ability.

7.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, pupils and visitors will read and sign the visitor acceptable use policy before being given access to our computer system, IT resources or internet.

7.3 Filtering and Monitoring

7.3.1 Decision making

- Foreland Fields School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders 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 pupils; effective classroom management and regular education about safe and responsible use is essential.
- We monitor internet and technology use taking place via all school provided devices and systems and regularly evaluate online safety mechanisms to ensure this policy is consistently applied. Full information about the appropriate filtering and monitoring systems in place are also detailed in our child protection policy. Any issues identified as a result of our monitoring approaches will be incorporated into our action planning.

7.3.2 Appropriate filtering

- At Foreland Fields School will do all we reasonably can to limit children's exposure to online harms through school provided devices, systems, platforms and networks. In line with the requirements of the Prevent Duty and KCSIE, we will ensure that appropriate filtering and monitoring systems are in place.
- This includes ensuring application of appropriate filtering and monitoring to both static content, as well as dynamic and AI-generated materials, products and/or systems used.
- Foreland Fields School's education broadband connectivity is provided through Medway Grid for Learning – Netsweeper. It:
  - is a member of Internet Watch Foundation (IWF).
  - has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU).
  - is blocking access to illegal content including child sexual abuse material (CSAM).
  - blocks access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content which promotes discrimination or extremism, drugs/substance misuse, malware/hacking, gambling, piracy and copyright theft, pro-self-harm, eating disorder and/or suicide content, pornographic content and violent material.
- Netsweeper blocks school provided internet access to illegal content and activity as identified in the Online Safety Act, including:
  - Child Sexual Abuse Material (CSAM)
  - Controlling or coercive behaviour
  - Extreme sexual violence
  - Extreme pornography
  - Fraud
  - Racially or religiously aggravated public order offences
  - Inciting violence
  - Illegal immigration and people smuggling
  - Promoting or facilitating suicide
  - Intimate image abuse
  - Selling illegal drugs or weapons
  - Sexual exploitation
  - Terrorism

- Netsweeper is a member of Internet Watch Foundation (IWF) and uses IWF services to block access to CSAM.
- Netsweeper has signed up to Counter-Terrorism Internet Referral Unit list (CTIRU)
- Netsweeper blocks school provided internet access to sites which could promote or include harmful and/or inappropriate behaviour or material. This includes content or activity which promotes hate speech or discrimination, gambling, harmful bullying content, malware/hacking, mis-disinformation, privacy and copyright theft, pornography, self-harm and eating disorders and/or violence against women and girls.
- Our filtering system is operational, up to date and applied to all users, including guest accounts, all school owned or provided devices, systems and networks, and all devices using the school internet connection.
- The DSL and Leadership Team will work with Medway Grid for Learning/Netsweeper and our IT Technicians to ensure that our filtering policy (found within school's Online Safety Policy) is continually checked and reviewed to reflect our needs and requirements.
- If there is failure in the software or abuse of the system, for example if pupils/students or staff accidentally or deliberately access, witness or suspect unsuitable material has been accessed, they are required to follow the procedures as set out in the school's Online Safety Policy.
- Filtering breaches will be reported to the DSL and technical staff and will be recorded and escalated as appropriate and in line with relevant policies, including our Child Protection, Acceptable Use, Allegations Against Staff and Positive Behaviour Policies.
- Parents/carers will be informed of filtering breaches involving their child.
- Any access to material believed to indicate a risk of significant harm, or that could be illegal, will be reported as soon as it is identified to the appropriate agencies, including but not limited to the Internet Watch Foundation (where there are concerns about child sexual abuse material), Kent Police, NCA-CEOP or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.
- If staff are teaching topics which could create unusual activity on the filtering logs, or if staff perceive there to be unreasonable restrictions affecting teaching, learning or administration, they will report this to the DSL and/or Leadership Team.
- The school has a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all pupils) will be made aware of. It has been shared with the staff team through training. This procedure includes taking the pupil away from the device and either locking the screen or turning it off and reporting the incident to the Deputy Designated Safeguarding Lead with responsibility for online safety. The breach will be recorded and escalated as appropriate. Parents will be informed of filtering breaches involving their child.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy) or headteacher/manager will seek advice from Kent County Councils Education Safeguarding Service or other agency in accordance with our child protection policy.
- If pupils discover unsuitable sites, they will be required to:
    - Turn off or lock the monitor/screen and report the concern immediate to a member of staff.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or Deputy) and/or technical staff.
    - The breach will be recorded and escalated as appropriate.
    - Parents/carers will be informed of filtering breaches involving their child.

7.3.3 Appropriate monitoring

- We will appropriately monitor the use of all school provided devices and networks to detect safeguarding risks in real or near-real time, including accessing or attempting to access, or engaging with or attempting to engage with illegal and/or harmful/inappropriate content or activity by any user. This is achieved by all school devices

including PCs, laptops, iPads, touchscreen devices and SMART/wearables having Netsweeper installed and operational, including at satellite provisions and during any off-site use. It is not possible for staff to disable Netsweeper. Staff receive training in filtering and monitoring and are instructed not to adjust settings. Staff are not able to access school Wifi using personal devices. Governors personal laptops/electronic devices are provided with a certificate that enables them to use the school Wifi however, their use is monitored in the same way as staff and pupils. Visitors are enabled to access Wifi via a temporary password issues by the IT Technician and, as such, all visitor internet searches are filtered and monitored. The school has an active Wifi acceptable use policy which is signed by all staff and visitors. Pupils, as appropriate, are taught about filtering and monitoring and, where possible, are aware that this is taking place. Netsweeper allows Foreland Fields School to identify device names or IDs, IP addresses, and individual users, the time and date of attempted access and the search term or content being blocked.

- All users will be informed that use of our devices and networks can/will be monitored and that all monitoring is in line with data protection, human rights and privacy legislation.
- If a concern is identified via our monitoring approaches:
  - Where the concern relates to pupils/students, it will be reported to the DSL and will be recorded and responded to in line with relevant policies, such as Child Protection, Acceptable Use, and Behaviour Policies.
  - Where the concern relates to staff, it will be reported to the Headteacher (or Chair of Governors if the concern relates to the Headteacher), in line with our Staff Behaviour Policy.
- Parents/carers will be informed of safeguarding concerns involving their child identified through our monitoring approaches, unless to do so would put a child at risk of harm or compromise a criminal investigation.
- Where our monitoring approaches detect any immediate risk of harm or illegal activity, this will be reported as soon as possible to the appropriate agencies; including but not limited to, the emergency services via 999, Kent Police via 101, NCA-CEOP , LADO or Kent Integrated Children's Services via the Kent Integrated Children's Services Portal.
- Whilst filtering and monitoring is an important part of our online safety responsibilities, it is only one part of our approach, and we recognise that we cannot rely on filtering and monitoring alone to safeguard our pupils/students. Effective safeguarding practice, robust policies, appropriate classroom/ behaviour management and regular education/ training about safe and responsible use is essential and expected.
  - Pupils/students will use appropriate search tools, apps and online resources as identified by staff, following an informed risk assessment and/or a data privacy impact assessment as relevant.
  - Internet use will be supervised by staff as appropriate to pupils/students age, ability and potential risk of harm.

7.3.4 Responsibilities for filtering and monitoring

- Our Governing Body has overall strategic responsibility for our filtering and monitoring approaches, including ensuring that our filtering and monitoring systems are regularly reviewed, and that the Leadership Team and relevant staff have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate safeguarding concerns when identified.
- Adrian Mount (DSL/Headteacher) and Steve Pamphilon (Chair of Governors), are responsible for ensuring that our school has met the DfE Filtering and monitoring standards for schools and colleges.
- Our Senior Leadership Team is responsible for:
  - procuring filtering and monitoring systems.
  - documenting decisions on what is blocked or allowed and why.
  - reviewing the effectiveness of our provision.
  - overseeing reports.
  - ensuring that all staff understand their role, are appropriately trained, follow policies, processes and procedures and act on reports and concerns.

    - ensuring the DSL, IT Technicians have sufficient time and support to manage their filtering and monitoring responsibilities.
- The DSL has lead responsibility for overseeing and acting on:
    - any filtering and monitoring reports.
    - any child protection or safeguarding concerns identified.
    - checks to filtering and monitoring system.
- The IT Technicians have technical responsibility for:
    - maintaining filtering and monitoring systems.
    - providing filtering and monitoring reports.
    - completing technical actions identified following any concerns or checks to systems.
    - working with the Senior Leadership Team and DSL to procure systems, identify risks, carry out reviews and carry out checks.

- All members of staff are provided with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of our induction process, and in our child protection staff training.
- All staff, pupils/students and parents/carers have a responsibility to follow this policy to report and record any filtering or monitoring concerns.

7.3.5 Decision making and reviewing our filtering and monitoring

- When procuring and/or making decisions about our filtering and monitoring provision, our Senior Leadership Team works closely with the DSL and the IT technicians.
- Decisions about our filtering and monitoring provision have been recorded and informed by an approach which ensures our systems meet our school needs and circumstances, including but not limited to our pupil/student risk profile which considers the specific vulnerabilities (including age and ability), risk and context of our pupils/students, and our school specific technology use.
- Any changes to the filtering and monitoring approaches will be assessed by staff with safeguarding, educational and technical experience and with approval from the Leadership Team; all changes to the filtering policy are logged and recorded.
- Our school undertakes regular (at least annual) reviews of our filtering and monitoring approaches to ensure we understand the changing needs and potential risks posed to our community.
- In addition, our school undertakes regular and active checks on our filtering and monitoring systems to ensure our systems work effectively in practice and as expected, and to provide assurance to the Governing Body that we are continuing to meet our safeguarding obligations. These checks are logged and recorded via Netsweeper and OnGuard.

  These checks are achieved by:
    - Daily reports of the previous day's activity.
    - Live reports from OnGuard.
    - Also see 6.3.3 below.
    - Headteacher, Deputy Headteacher and It Technicians check reports daily and these are discussed wider as part of regular Online Safety meetings.
    - Online Safety concerns discussed in weekly meetings. Online Safety is a weekly agenda item.
    - Any concerns raised through filtering and monitoring are dealt with on a risk assessment basis. Where there is a risk of harm, matters are dealt with immediately.

7.4 Managing personal data online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection regulation.

- Full information can be found in our data legislation compliant information Governance system on KLZ. In particular, for full detail, staff should refer to the School data protection, data handling security and acceptable personal use of resources and assets policies.

7.5 Security and management of information systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Anonymisation of documents and minimisation of data.
  - Encryption and passwords for personal data sent over the Internet (this may include use of software such as egress switch) or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Preventing, as far as possible, access to websites or tools which could compromise our systems, including anonymous browsing and other filtering bypass tools.
  - Regularly checking files held on our network, the Network manager will regularly check system capacity.
  - The appropriate use of user logins and passwords to access our network.
  - Specific user logins and passwords will be enforced for all but the youngest and least able users.
  - All users are expected to log off or lock their screens/devices if systems are unattended.

7.5.1 Password policy

- All users will be informed not to share passwords or information with others and not to login as another user at any time.
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it. As appropriate and dependent on pupil ability / needs staff will have access to pupil passwords to support their access to computers.
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- From February 2017, all pupils were provided with their own unique username and passwords to access school systems.
- We require staff to use STRONG passwords for access into our system.
- We require pupils to use passwords of a strength appropriate to their level of need (ability to remember and enter the password). In some cases, this will be a generic password.
- We require staff to change their passwords every 6 months.

7.6 Managing the safety of our website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

7.7 Publishing images and videos online – including YouTube

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones (both within this policy and the Mobile Phone and Smart Technology Policy).
- In line with the school's image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published, for example: YouTube, school website or ClassDoJo (but not in the case of applications which enable the school to perform its public duty, for example Evidence for learning).
- The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have either recorded themselves or have downloaded from the internet.
- However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may potentially cause significant harm or embarrassment to individuals in the short or longer term.
- All members of staff (including volunteers) will ensure that all images are available for scrutiny and will be able to justify any images in their possession.
- Images or videos that include children will be selected carefully for use e.g. only using images of children who are suitably dressed.
- No group photos are shared with parents /carers on ClassDojo, whole school or class story– individual images only on individual messaging or individual portfolio. Evidence for learning and Seesaw also only use individual pupil image when sharing with parents/carers.
- The school has a YouTube channel. This is called Foreland Fields School. It is administrated by the Deputy Headteacher with responsibility for Online Safety. It is used to create Teaching and Learning opportunities for pupils and to provide training opportunities for Staff, Parents/carers and the wider professional school network. Also, to celebrate pupil achievement. All videos are checked and uploaded by the DHT.

7.7.1 SeeSaw, ClassDoJo and Evidence for Learning

- The school uses Seesaw, ClassDoJo and Evidence for Learning to upload and share images of children with parents for both assessment and celebration purposes. Photos are only shared directly to individual parents/carers and never to whole classes / whole school.
- School will seek consent for us of image for ClassDoJo as this is used for celebration purposes. It will inform parents of its use of image on Seesaw and Evidence for Learning, as this is part of its statutory duty to assess pupil progress and consent is not required.
- Parents may share appropriate pupil images from home learning directly with teachers (and not with the whole class) via Seesaw and ClassDojo. The teacher should then not share this image from home with the wider class group.
- The use of these sites has been appropriately risk assessed by the Online Safety Lead / the DPO. The governing body and Headteacher have taken steps to ensure all data stored is held in accordance with data protection law.
- Pupil Images uploaded to Seesaw, ClassDoJo and Evidence for learning will only be taken on school/setting devices. These images will then be uploaded to the sites, then deleted from the school device.
- Staff and SLT may upload appropriate images / video of themselves onto ClassDoJo Class story / school story as part of their communication / interaction within the class, during term time, but also, especially during long periods away from school e.g. summer holidays, school lockdown. They can use their own mobile devices to do this.
- All users of Seesaw, ClassDoJo and Evidence for learning are advised on safety measures to protect all members of the community e.g. using strong passwords, logging out of systems after use etc.
- Parents/carers will be informed of the school/settings expectations regarding safe and appropriate use (e.g. not sharing passwords or copying and sharing images) prior to being given access. Failure to comply with this may result in access being removed.
- The pupil's images on these sites will be deleted on request of parents, in accordance with data protection law, this will occur one year after the end of the pupil's school career, in line with the agreed data retention policy (see Information Governance Framework).
- The Online Safety Lead and Network Manager have checked the privacy policy and conducted data impact risk assessments of each of these Apps as per the Information Governance Framework.

7.8 Managing email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
    - The forwarding of any chain messages/emails is not permitted.
    - Spam or junk mail will be blocked and reported to the email provider.
    - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.

- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell (Adrian Mount, Designated Safeguarding Lead and Online Safety Lead) if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- 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.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

7.8.1 Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

7.8.2 Pupil's email

- Pupils will use provided email accounts for educational purposes.
- Pupils will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

7.9 Educational use of Videoconferencing, Webcams and Video Chat /document sharing Apps (Microsoft teams for staff/ professionals/multi-agency).

- The school does not currently have a bespoke video conferencing facility and does not participate in use of video conferencing or webcam use. All staff laptops and school iPads are controlled by the IT manager to ensure that webcams and video conferencing capabilities are not enabled.
- Should an educational event arise in the future that warrants the use of video conferencing or webcams then the following policy statements will apply.
- Foreland Fields School recognise that video conferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All video conferencing and webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Video conferencing 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.
  - Video conferencing contact details will not be posted publicly.
  - Video conferencing equipment will not be taken off the premises without prior permission from the DSL.

- Staff will ensure that external video conferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

- In response to the COVID-19 crisis and moving forwards, to prepare students for future life Foreland Fields School now allows staff and students to use Microsoft Teams – video conferencing. In the case of Microsoft Teams this is to enable some social learning opportunities during this prolonged period of isolation and also virtual meetings to take place such as EHCP reviews and CiC meetings to take place. The Online Safety Lead and Network Manager have checked the privacy policy and conducted data impact risk assessments as per the Information Governance Framework.
- Microsoft Teams has been chosen as it is are password protected and encrypted**,** Staff and parents are allowed to use their own mobile devices as well as school devices to support the App, the following measures must be followed to maintain safety;
  - Specific written consent must be gained from parents.
  - Parents must be present at all times during video chat.
  - Two members of staff (one of whom must be a Teacher) must be present at all times during the video chat. At least two pupils must be present in the chat (no 1:1 video chat).
  - The video chat must be pre-planned and purposeful in line with the pupil's curriculum.
  - Only Teachers can plan and lead a video chat session and they must gain permission from their Leader of Learning AND the Online Safety Lead.
  - The video call MUST NOT be recorded. Log out after use.
  - If the school decides to record a live session consent must be first gained from SLT and then from all participants.
  - The success of the video call should be reviewed and feedback provided to the Leader of Learning.
  - Staff should dress professionally and use a neutral background for their video stream.
  - Staff should consider reducing live camera time e.g. sharing PowerPoint and video. Staff should check all pre-recorded content prior to sharing. If required SLT could review content prior to sharing.
  - Ensure staff have control over the student's video/audio functionality.
  - Where possible staff should restrict student access to chat/video functions once a live session has ended.
  - SLT will monitor a selection of remote sessions to check they are being conducted appropriately.
  - Staff and pupils/students will be encouraged to report issues experienced at home when participating in remote/online learning; concerns will be responded to in line with our child protection and other relevant policies.

7.9.1 Video Conferencing Users

- Parents/carers consent will be obtained prior to pupils taking part in video conferencing activities.

- Pupils will ask permission from a member of staff before making or answering a video conference call or message.
- Video conferencing will be supervised appropriately, according to the pupil's age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to video conferencing administration areas or remote-control pages.
- The unique log on and password details for the video conferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.
- Pupils and supervising parents/carers should wear appropriate clothing and use a neutral background with no other siblings/family members in the background.
- Students should be supervised throughout the live stream.
- Pupils should behave as they would in the classroom.

7.9.2 Video conferencing content

- When recording a video conference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a video conference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the pupils.

7.10 Management of learning platforms - Seesaw

- The IT manager, SLT and staff will regularly monitor the usage of the LP (KLZ and purple mash, Seesaw, are used currently) by staff and pupils in all areas, in particular message and publishing facilities.
- Seesaw is a learning platform which enables teachers to upload lesson content, including video explaining tasks, eBooks, PowerPoints, learning resources etc. With the support of their parents/carers, pupils can then access this virtual classroom to improve remote and home learning. Parents can upload video/images of pupils competing tasks, but teachers should give guidance as to whether it is best to upload on Seesaw, Evidence for learning or both.
- The Online Safety Lead and Network Manager have checked the privacy policy conducted data impact risk assessments of each of these Apps as per the Information Governance Framework.
- As Teaching and Learning is part of the school's public duty it only needs to inform parents of the use of Seesaw.
- Staff and pupils will be advised about acceptable conduct and use when using the LP.
- Only members of the current pupil and staff community will have access to the LP.

- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc. leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns about content on the LP may be recorded and dealt with in the following ways:
  a) The user will be asked to remove any material deemed to be inappropriate or offensive.
  b) The material will be removed by the site administrator if the user does not comply.
  c) Access to the LP for the user may be suspended.
  d) The user will need to discuss the issues with a member of leadership before reinstatement.
  e) A pupil's parent/carer may be informed.
- A visitor may be invited onto the LP by a member of the leadership. In this instance there may be an agreed focus or a limited time slot.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

7.11 Management of applications (apps) used to record children's progress - Evidence for Learning

- The school uses Evidence for Learning to track pupil's progress and share appropriate assessment information with parents and carers. This includes sharing videos/images of pupils working directly with parents/carers/social workers.
- Evidence for Learning are used for assessment purposes. Data protection law allows for assessment data to be processed under the legal basis of public task rather than requiring consent. The school is still required to let individuals know that it uses the systems within its privacy notice.
- 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.
- In order to safeguard pupil'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 children's personal details, attainment or images.
  - School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents can upload images and video to Evidence for Learning in order to contribute to the pupil's holistic assessment.

7.12 Remote working – Ivanti secure access

Remote working (accessing school IT systems and data from a remote location) via ~~Pulse secure~~ (Ivanti Secure Access Client) has been recommended by EIS and is now the schools adopted method of remote working.

- Using a remote-access VPN connection (Virtual Private Network) individual staff members may now securely connect to the school network from a remote location using a laptop or desktop computer connected to the internet.
- Remote access is available to all members of SLT (open access) and Teachers (on request and approval by SLT).
- The following steps must be taken to enable a secure and robust connection:

- Staff members must be added to the school's VPN Security Group. (Staff are added/removed in the 'User Management Tool' by an IT Network administrator.)
- 'Ivanti Secure Access Client' software must be installed on the hardware device to be used for remote working. Ivanti Secure Access Client provides the secure, authenticated access for remote and mobile users.
- A KPSN School SSL VPN username login and password must be provided by the school's IT Network Manager or other school Network administrator.
- The IT Network Manager has created a Remote Desktop Connection using Microsoft Terminal Services Client (MSTSC) and network access has been enabled.

Once set up for remote working staff must follow all related school policies, including this Online Safety Policy, Data Protection Policy, Staff Acceptable Use Policy, data Handling and Security Policy. Specifically, but not limited to the following guidance; maintaining secure passwords, working in a private space when at home (not observable by others), logging out when not using the computer.

The staff must all refer to and follow the data handling and security policy which is which is within the Information governance system and is published on Office SharePoint.

7.13 Use of IRIS to support staff development.

- IRISConnect is to be used to support staff development and training. It will be used to record lessons and learning opportunities with a focus on the pedagogy employed by the class staff.
- The IRISConnect site has been risk assessed by the DPO with all necessary changes to GDPR records/audits made.
- Use/storage of video and image on this system is on the basis of the school's public duty and as such staff and parents/carers are notified, consent does not need to be sought.
- Staff using IRISConnect will use it purely for CPD purposes in a positive and solution focussed manner in line with the schools coaching policy.
- All videos and analysis uploaded to the system will reflect the school staff behaviour policy and uphold high standards of professionalism and maintain the integrity of the school's reputation.

7.14 Use of music streaming apps and voice control technology

- The use of any App must be approved by the DHT/HT and then assessed by the network manager and/or EIS. Only the Network manager should place any App (including Music Apps) on the school mobile devices
- Music streaming Apps such as Spotify can be used via school mobile devices such as iPads, but not through staff personal devices.
- The official school accounts can be used rather. Personal accounts cannot be used.

- Passwords for these accounts should be kept for staff only.
- Staff must preview music content for appropriateness prior to playing.
- School finance details will not be saved on the account settings of any App being used. An appropriate generic address and password following the school online safety policy will be used.
- Voice control technology using hardware such as Amazon Echo and Google Nest can be used following approval of the DHT/HT and where it is used solely as a tool to deliver the school's curriculum and intent – promoting independent living.
- Any device used must be purchased by the school with the approval of the DHT and following assessment by the Network manager and/or EIS.

7.15 Use of MyConcern to record safeguarding concern

- See also section 10 – responding to online safety incidents and concerns.
- MyConcern is used to record all safeguarding concerns at the school. MyConcern is a secure software platform designed for schools to record, manage and track safeguarding and wellbeing concerns for students and staff. It is used nationally and internationally and is recognised as a secure system. The system has been approved by the schools Data Protection Officer. All staff have received training in use of this system and have their own login details.

7.16 Use of IRISAdapt to record accidents, behaviour incidents, medical incidents and errors in the administration of medication

- IRISAdapt is a secure and configurable data management application that is used nationally. The school currently uses it to record accidents, behaviour incidents, medical incidents and errors in the administration of medication. The system has been approved by the schools Data Protection Officer. All staff have received training in use of this system and have their own login details.

7.17 Generative Artificial Intelligence (AI)

- Foreland Fields School recognises that when used safely, effectively and with the right infrastructure in place, generative artificial intelligence (AI) tools have many uses which could benefit our entire school community.
- However, it is important to recognise that AI tools can also pose safeguarding risks to our community as well as moral, ethical and legal concerns. This includes, but is not limited to:
  - exposure to inappropriate or harmful content, including bullying, harassment, abuse and exploitation
  - privacy and data protection breaches/risks
  - intellectual property infringements
  - academic integrity challenges such as plagiarism and cheating
  - exposure to inaccurate, misleading, or biased content.
- Foreland Fields School only permits the use of generative AI tools which have been approved and provided by the school for work and/or educational purposes, following the Senior Leadership Team undertaking risk assessments and/or data protection impact assessments prior to use.
- Staff and pupils/students will be made aware of the benefits and risks of using generative AI tools and the school expectations by ensuring they have access to and read the Child Protection and Online Safety Policies and covering AI use in staff training sessions.

- Foreland Fields School will respond to any misuse of AI in line with relevant policies, including but not limited to, anti-bullying, behaviour, data protection, complaints and child protection.
- Where the School believe that AI tools may have facilitated the creation of child sexual abuse material, the school will respond in line with existing local safeguarding procedures and national guidance from the IWF and NCA-CEOP.
- Where the School are responding to concerns regarding digitally manipulated and AI-generated nudes and semi-nudes, the school will respond in line with section 4.3 of this policy and the local KSCMP safeguarding procedures and UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance.

- Where the school believe that AI tools may have facilitated deep fake abuse of adults, advice and support will be provided to individuals affected, such as via Unions, Professionals Online Safety Helpline or Report Harmful Content and/or if a crime has been committed, via the police. Action will be taken in line with relevant school policies, including but not limited to, Anti-Bullying, Positive Behaviour and Complaints.

8. Social Media

8.1 General social media expectations

- Foreland Fields School believes 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 Foreland Fields School community are expected to engage in social media in a positive and responsible manner.
- All members of the Foreland Fields School community are advised not to post or share content that may be considered threatening, hurtful or defamatory to others on any social media service.
- We will control learner and staff access to social media via our filtering and monitoring systems which are applied to all school provided devices and systems; further information on how this is achieved in addressed in our child protection policy.
- Inappropriate or excessive use of social media during Foreland Fields School hours or whilst using Foreland Fields School devices may result in removal of internet access and/or disciplinary action.
- The use of social media or apps, for example as a formal remote learning platform will be robustly risk assessed by the DSL/Headteacher prior to use. Any use will take place in accordance with the details laid out in this policy.
- Concerns regarding the online conduct of any member of Foreland Fields School community on social media will be taken seriously. Concerns will be managed in accordance with the appropriate policies, including anti-bullying, allegations against staff, behaviour, home school-agreements, staff behaviour/code of conduct, Acceptable Use Policies, and child protection.

8.2 Staff personal use of social media

- The use of social media during school/setting hours for personal use is only permitted for staff at break time, in the staffroom and using their own mobile/smart device in accordance with the staff AUP's and all other Online Safety and safeguarding policies.
- Safe and professional online behaviour is outlined for all members of staff, including volunteers, as part of our code of conduct/behaviour policy and/or acceptable use of technology policy.

- The safe and responsible use of social media sites will be discussed with all members of staff as part of staff 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. Amend as appropriate.
- Any complaint about staff misuse of social media or policy breaches will be taken seriously in line with our child protection and allegations against staff policy.

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 location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the setting.
- Members of staff are encouraged not to identify themselves as employees of Foreland Fields School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, 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 pupils 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 any content shared on social media sites conflicts with their role.

Communicating with pupils and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL and/or the Deputy DSL (responsible for online safety). Decisions made and advice provided in these situations will be formally recorded in order to safeguard pupils, the setting and members of staff.

- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or Deputy). Decisions made and advice provided in these situations will be formally recorded to safeguard pupils, members of staff and the setting.
- ClassDojo has been put in place as a safe, education based site which enables communication between parents and staff.

8.3 Pupil's use of social media

- The use of social media during school hours for personal use is not permitted for pupils, except where part of teaching and learning about online safety and social media.
- Many online behaviour incidents amongst children and young people occur on social media outside the school day and off the school premises. Parents/carers are responsible for this behaviour; however, some online incidents may affect our culture and/or 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 pupil, could have repercussions for the orderly running of the school when the pupil 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.
- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Foreland Fields School will empower our pupils 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 pupils 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.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for pupils under this age as outlined in the services terms and conditions.
- Any concerns regarding pupils use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
    - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Pupils will be advised:
    - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
    - To only approve and invite known friends on social media sites and to deny access to others, for example by making profiles private.

- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

- Sanctions, but most probably, pastoral/welfare support will be implemented and offered to Pupils as appropriate, in line with our child protection and behaviour policies. Civil or legal action will be taken if necessary, but within our context, this is unlikely.

8.4 Official use of social media - ClassDojo

- Foreland Fields School official social media channel is ClassDojo
- The official use of ClassDojo only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- ClassDojo has been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage ClassDojo.
  - ClassDojo is suitably protected.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- ClassDojo use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
  - All communication on official ClassDojo will be clear, transparent and open to scrutiny.
- Parents/carers and pupils will be informed of any official ClassDojo use, along with expectations for safe use and action taken to safeguard the community. Parents sign an agreement document outlining safe and appropriate use of ClassDojo.
  - Only ClassDojo which has been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving pupils will be moderated possible.
- Parents and carers will be informed of any official social media use with pupils; 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.

Staff expectations

- 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 participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our acceptable use policy, which details social media use.
  - Be professional, responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
  - Always be professional and aware they are an ambassador for the setting.
  - Disclose their official role and position but make it clear that they do not necessarily speak on behalf of the setting.
  - Always be 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 this policy as well as our use of image policy, ensuring that they have appropriate consent before sharing images on the official social media channel. If they wish, Teachers can share video/images of themselves on ClassDoJo via the class story function – this would be to support teaching and learning and/or social/emotional development. Teachers can share images/video of **individual** pupils via the direct messaging function or individual pupil portfolio, but not on the class story function. These images /videos must not have other pupils in the background. Full consent must be gained prior to doing this. SLT may share videos/photos of themselves on whole school story, but must not share images of pupils on whole school story – unless with specific consent from parents. Parents can share appropriate video/image of their child with the class teacher on ClassDojo via the direct message function.
  - Staff may use their personal mobile devices to upload messages and images/videos of themselves to class story and parent messaging.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - The direct messaging function between Teachers / SLT and parents can be used on ClassDoJo.
  - Inform their line manager, the DSL (or Deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from pupils.
  - Staff should be aware that the DSL can (on request to the ClassDojo administrator (if required, due to allegations/complaints from a Teacher or parent/carer) access all messaging streams on Dojo.

9. Use of Mobile and Smart Technology

- See Foreland Field's School's Mobile Phone and Smart Technology Policy.

- Foreland Fields School recognises that personal communication through mobile and smart technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.
- Foreland Fields School recognises the specific risks that can be posed by mobile and smart technology, including mobile/smart phones, cameras, wearable technology and any other electronic devices with imaging and/or sharing capabilities.

9.1 Expectations

- Staff, parent/carers and pupils should refer to and follow the guidance in the Staff Behaviour Policy and in the school mobile phone policy.

9.2 Staff use of mobile and smart technology

- Staff should refer to and follow the guidance in the staff behaviour policy and in the school's Mobile Phone and Smart Technology Policy.

9.3 Pupil's use of mobile and smart technology

- In the first instance staff and parents should refer to the school's Mobile Phone and Smart Technology Policy. In line with this guidance all students' mobile phones are held by class teachers for the duration of the school day.

9.4 Visitors' (including parents) use of mobile and smart technology

- Parents/Carers and staff should in the first instance refer to the Schools Mobile Phone and Smart Technology Policy

9.5 Officially provided mobile phones and devices including GPS trackers

- Refer to the school's Mobile Phone and Smart Technology Policy.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying or online abuse, material related to radicalisation and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
    - Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

- If we are unsure how to proceed with an incident or concern, the DSL (or Deputy DSL responsible for online Safety) will seek advice from the Education Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Education Safeguarding Team or Kent Police using 101, or 999 if there is immediate danger or risk of harm.
- If information relating to a specific incident or a concern needs to be shared beyond our community, for example if other local settings are involved or the wider public may be at risk, the Headteacher (DSL) will speak with the police and/or the Education Safeguarding Service first, to ensure that potential criminal or child protection investigations are not compromised.

10.1 Concerns about children/pupil/student welfare

- The DSL (or Deputy) will be informed of all online safety concerns involving safeguarding or child protection risks in line with our child protection policy (reporting via MyConcern and in person to the DSL (or Deputy) as soon as practically possible if there is risk of immediate harm).
- All concerns about pupils will be recorded in line with our child protection policy.
- Foreland Fields School recognises that whilst risks can be posed by unknown individuals or adults online, pupils can also abuse their peers; all online child on child abuse concerns will be responded to in line with our child protection and behaviour policies.
- The DSL (or Deputy) will ensure that online safety concerns are escalated and reported to relevant partner agencies in line with local policies and procedures.
- Appropriate sanctions and/or pastoral/welfare support will be offered to pupils as appropriate. Civil or legal action will be taken if necessary.
- We will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

10.2 Concerns about staff online behaviour and/or welfare

- Any complaint about staff misuse will be referred to the Headteacher in accordance with our allegations against staff policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate disciplinary, civil and/or legal action will be taken in accordance with our staff behaviour policy/code of conduct.
- Welfare support will be offered to staff as appropriate.

10.3 Concerns about parent/carer online behaviour and/or welfare

- Concerns regarding parents'/carers behaviour and/or welfare online will be reported to the Headteacher and/or DSL (or Deputy) (reporting via MyConcern and in person to the DSL (or Deputy) as soon as practically possible if there is risk of immediate harm).

- The Headteacher and/or DSL will respond to concerns in line with existing policies, including but not limited to child protection, anti-bullying, complaints, allegations against staff, home-school agreements, acceptable use of technology and behaviour policy.
- Civil or legal action will be taken if necessary.
- Welfare support will be offered to parents/carers as appropriate.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online sexual violence and sexual harassment between children

- Our Headteacher, DSL and appropriate members of staff have accessed and understood the DfE "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2021.
  - Full details of our response to child on child abuse, including sexual violence and harassment can be found in our child protection policy.
- Foreland Fields School recognises that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Amongst other things, this can include widespread abuse or harm across a number of social media platforms that leads to repeat victimisation.
- Foreland Fields 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
  - Coercing others into sharing images of themselves of performing acts they're not comfortable with.
- 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 (reporting via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.
  - if content is contained on pupils personal devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.

- provide the necessary safeguards and support for all pupils 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 Work Service 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.
- review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

- Foreland Fields 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.
- Foreland Fields School recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- To help minimise concerns, Foreland Fields 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 pupils.

11.2 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 18. 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.

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, and should be read and understood by DSLs working will all age groups, not just older pupils.

- Foreland Fields 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, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, 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 as set out in 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.

11.3 Online child sexual abuse and exploitation (including child criminal exploitation)

- Foreland Fields 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.
- Foreland Fields 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 DSL responsible for online safety). Reporting will be via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.
- 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 pupils, 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 pupils and other members of our community.
- 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 Safeguarding Child Board's procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to Children's Social Work Service (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 pupils, 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, pupils 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 DSL responsible for online safety) 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 police by the DSL (or Deputy DSL responsible for online safety).
- If pupils at other setting are believed to have been targeted, the DSL (or Deputy DSL responsible for online safety) will seek support from Kent Police and/or the Education Safeguarding Team first to ensure that potential investigations are not compromised.

11.4 Indecent images of children (iioc)

- Foreland Fields 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 we are unclear if a criminal offence has been committed, the DSL (or Deputy DSL responsible for online safety) 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 Safeguarding Child Boards 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 learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or Deputy DSL responsible for online safety) is informed.
  - Reporting will be via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.
  - 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 (or Deputy DSL responsible for online safety) 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.

11.5 Cyberbullying and cybercrime/commerce

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Foreland Fields School.
- Reporting will be via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.
- Foreland Fields School recognises that children with particular skill and interest in computing and technology may inadvertently or deliberately stray into 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer/internet enabled device) cybercrime.
- If staff are concerned that a child may be at risk of becoming involved in cyber-dependent cybercrime, the DSL will be informed, and consideration will be given to accessing local support and/or referring into the Cyber Choices programme, which aims to intervene when young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.
- Where there are concerns about 'cyber-enabled' crime such as fraud, purchasing of illegal drugs online, child sexual abuse and exploitation, or other areas of concern such as online bullying or general online safety, they will be responded to in line with this and other appropriate policies.

11.6 Online hate

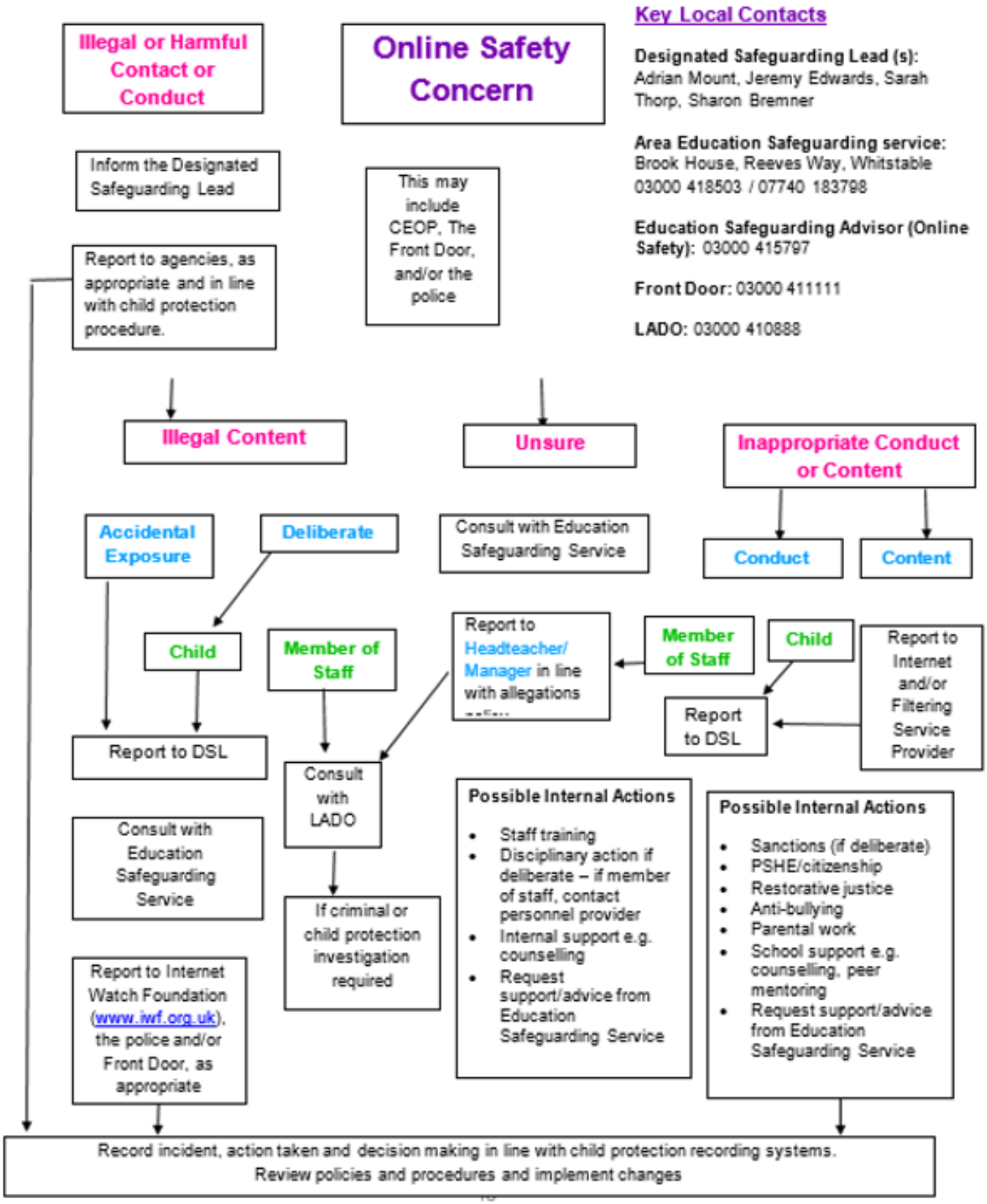
- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Foreland Fields School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- Reporting will be via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.
- 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 (or Deputy DSL responsible for online safety) will obtain advice through the Education Safeguarding Team and/or Kent Police.

11.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. See section 7.3 on filtering and monitoring.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or Deputy DSL responsible for online safety) will be informed immediately, and action will be taken in line with our child protection policy.
- Reporting will be via MyConcern and in person to the DSL (or Deputy), as soon as is practically possible if there is risk of immediate harm.

- If we are concerned that 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.

Responding to an Online Safety Concern Flowchart



12. Useful Links for Educational Settings

Kent Educational Setting Support and Guidance

Education Safeguarding Service, Kent County Council:

- 03000 415797
  - Rebecca Avery, Education Safeguarding Advisor (Online Protection)
  - Ashley Assiter, Online Safety Development Officer
- 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

KSCMP: https://www.kscmp.org.uk/
UKCIS guidance: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

Kent Police:

- www.kent.police.uk or www.kent.police.uk/internetsafety
- In an emergency (a life is in danger or a crime in progress) dial 999. For non-urgent enquiries, contact Kent Police via 101

Front Door:

- The Front Door can be contacted on 03000 41 11 11
- Out of hours (after 5pm / Urgent calls only) please contact: 03000 41 91 91

Early Help and Preventative Services: www.kelsi.org.uk/special-education-needs/integrated-childrens-services/early-help-contacts

Other:

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

National Links and Resources for Settings, Pupils 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-and-professionals
  - 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