

**Foreland Fields School**

**Online Safety Policy**

**Governing Body Approval and Categories**

|  |  |
| --- | --- |
| Date of Last Review / Scrutiny | 7th October 2019 |
| Date (Month / Year) of Next Review /Scrutiny | October 2020 |
| Date Policy was Ratified | 9th October 2019 |
| Category of the Policy | Safeguarding |
| Named Lead for Writing the Policy | Jeremy Edwards – DHT |
| Named Governor for Scrutiny | Jason Gerlack |
| 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 |

|  |
| --- |
| **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

**Foreland Fields School**

**September 2019**

****

**Contents**

|  |  |
| --- | --- |
|  | **Page no** |
| Using the Online Safety Policy Template | 3 |
| 1. Policy Aims | 5 |
| 2. Policy Scope | 5 |
| 2.2 Links with other policies and practices | 6 |
| 3. Monitoring and Review | 6 |
| 4. Roles and Responsibilities | 6 |
| 4.1 The leadership and management team | 6 |
| 4.2 The Designated Safeguarding Lead | 7 |
| 4.3 Members of staff | 8 |
| 4.4 Staff who manage the technical environment | 8 |
| 4.5 Learners | 8 |
| 4.6 Parents | 9 |
| 5. Education and Engagement Approaches | 9 |
| 5.1 Education and engagement with learners | 9 |
| 5.2 Vulnerable Learners | 10 |
| 5.3 Training and engagement with staff | 10 |
| 5.4 Awareness and engagement with parents | 11 |
| 6. Reducing Online Risks | 11 |
| 7. Safer Use of Technology | 12 |
| 7.1 Classroom Use | 12 |
| 7.2 Managing Internet Access | 13 |
| 7.3 Filtering and Monitoring | 13 |
| 7.4 Managing Personal Data Online | 14 |
| 7.5 Security and Management of Information Systems | 14 |
| 7.6 Managing the Safety of the Website | 15 |
| 7.7 Publishing Images and Videos Online | 15 |
| 7.8 Managing Email | 15 |
| 7.9 Educational use of Videoconferencing and/or Webcams | 16 |
| 7.10 Management of Learning Platforms | 17 |
| 7.11 Management of Applications (apps) used to Record Learners Progress | 18 |
| 8. Social Media | 18 |
| 8.1 Expectations | 18 |
| 8.2 Staff Personal Use of Social Media | 19 |
| 8.3 Learners Personal Use of Social Media | 20 |
| 8.4 Official Use of Social Media | 21 |
| 9. Use of Personal Devices and Mobile Phones | 22 |
| 9.1 Expectations | 22 |
| 9.2 Staff Use of Personal Devices and Mobile Phones | 23 |
| 9.3 Learners Use of Personal Devices and Mobile Phones | 23 |
| 9.4 Visitors’ Use of Personal Devices and Mobile Phones | 24 |
| 9.5 Officially provided mobile phones and devices | 24 |
| 10. Responding to Online Safety Incidents and Concerns | 25 |
| 10.1 Concerns about Learner Welfare | 25 |
| 10.2 Concerns about staff onlinebehaviour/welfare 10.3 Concerns about parent/carer online behaviour and/or welfare | 25 |
| 11. Procedures for Responding to Specific Online Incidents or Concerns | 26 |
| 11.1 Online Sexual Violence and Sexual Harassment between Children | 26 |
| 11.2 Youth Produced Sexual Imagery or “Sexting” | 27 |
| 11.3 Online Child Sexual Abuse and Exploitation | 28 |
| 11.4 Indecent Images of Children (IIOC) | 29 |
| 11.5 Cyberbullying | 30 |
| 11.6 Online Hate | 30 |
| 11.7 Online Radicalisation and Extremism | 31 |
| 12. Useful Links for Educational Settings | 32 |

**Disclaimer**

The Education People make every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by The Education People. However, educational settings that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the Education People copyright is acknowledged and we are informed of its use.

****

# Foreland Fields School

# Online Safety Policy

**Key Details**

**Designated Safeguarding Lead (s): Adrian Mount, Headteacher**

**Deputy DSL with responsibility for Online Safety: Jeremy Edwards**

**Named Governor with lead responsibility: Jason Gerlack**

**Date written: October 2019**

**Date agreed and ratified by Governing Body: 9th October 2019**

**Date of next review: October2020**

**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, learners, Governors and parents/carers, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
* It takes into account the DfE statutory guidance ‘[Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)’ 2019, [Early Years and Foundation Stage](https://www.gov.uk/government/publications/early-years-foundation-stage-framework--2) 2017 ‘[Working Together to Safeguard Children](https://www.gov.uk/government/publications/working-together-to-safeguard-children--2)’ 2018 and the [Kent Safeguarding Children Board](http://www.kscb.org.uk) procedures.
* The purpose of Foreland Fields School online safety policy is to:
	+ Safeguard and protect all members of Foreland Fields School community online.
	+ Identify approaches to educate and raise awareness of online safety throughout the community.
	+ Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
	+ 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 three areas of risk:
	+ **Content:** being exposed to illegal, inappropriate or harmful material
	+ **Contact:** being subjected to harmful online interaction with other users
	+ **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
1. **Policy Scope**
* Foreland Fields School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners 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 learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
* This policy applies to 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) as well as learners, parents and carers.
* This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as a work laptops, tablets or mobile phones.

**2.2 Links with other policies and practices**

* This policy links with several other policies, practices and action plans including:
* Anti-bullying policy
* Acceptable Use Policies (AUP) and the staff code of conduct
* Behaviour and discipline policy
* Child protection policy
* Confidentiality policy
* Parent complaints procedure
* Relationships and sex education policy
* Safeguarding policy
* Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE), including online hate, radicalisation and extremism.
* Image use policy
* Information Governance Framework, including the data protection policy
1. **Monitoring and Review**
* Technology in this area evolves and changes rapidly. Foreland Fields School will review this policy at least annually.
	+ The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
* We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
* To ensure they have oversight of online safety, the Headteacherwill 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.
* Any issues identified via monitoring will be incorporated into our action planning.
1. **Roles and Responsibilities**
* The Designated Safeguarding Lead (DSL) (Adrian Mount, Headteacher) has lead responsibility for online safety. Whilst Online Safety operation and strategy is delegated to Jeremy Edwards (Deputy Designated Safeguarding lead and Lead for Online Safety), overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.
* 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.
* Ensure that online safety is embedded within a progressive curriculum, which enables all learners 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 Deputy Designated Safeguarding Lead / online safety lead delegated by the Designated Safeguarding Lead will:**

* 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 appropriate referrals are made to relevant external partner agencies, as appropriate.
* Work alongside the DSL and deputy DSLs to 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 learners 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 learners with SEN and disabilities (SEND) face online.
* 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.
* 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, the entire Online safety team, which comprises the Deputy DSL with responsibility for Online Safety, 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.

**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 policy is 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 learners (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.
* 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.
1. **Education and Engagement Approaches**

**5.1 Education and engagement with learners**

* 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](https://www.gov.uk/government/publications/education-for-a-connected-world)’ and DfE ‘[Teaching online safety in school](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)’ 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 learners 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 learners 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 learners who may be impacted by the content.
	+ making informed decisions to ensure that any educational resources used are appropriate for our learners.
	+ using external visitors, where appropriate, to complement and support our internal online safety education approaches. Staff can refer to‘[*Using External Visitors to Support Online Safety Education: Guidance for Educational Settings*](https://www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings)*.*
	+ rewarding positive use of technology.
* Foreland Fields School will support learners 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 learners 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 learners 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 learners 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 Learners**

* Foreland Fields School recognises that some learners 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 learners. 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.
* 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.
* 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 learners (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 learners.
* Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, 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 by:
	+ 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.
1. **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.
1. **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 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 i-pads 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 learners 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;
1. Pupils’ access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the pupils’ age and ability.

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, learners and visitors will read and sign an 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 learners; effective classroom management and regular education about safe and responsible use is essential.

**7.3.2 Appropriate Filtering**

* The school’s internet access strategy will be dependent on the need and requirements of our community and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff.
* The school uses educational filtered secure broadband connectivity through the KPSN which is appropriate to the age and requirement of our pupils.
* The school uses Light Speed filtering system which blocks sites that fall into categories such as pornography, racial hatred, extremism, gaming, sites of an illegal nature, etc.
* The school will ensure that age and ability appropriate filtering is in place whilst using school devices and systems to try and prevent staff and pupils from being accidentally or deliberately exposed to unsuitable content.
* The school will work with KCC and the Schools Broadband team or broadband/filtering provider to ensure that filtering policy is continually reviewed.
* 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.The procedure is clearly displayed in the staff room and computing room. 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.
* The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.
* Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Leadership Team.
* All changes to the school filtering policy will be logged and recorded.
* The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate.
* If learners 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.
* Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Kent Police or CEOP.

**7.3.4 Appropriate Monitoring**

* The school will appropriately monitor internet use on all school owned or provided internet enabled devices. In the majority of occasions this is achieved through physical monitoring (supervision), but a daily internet activity report and a suspicious search report is sent through EIS. This is monitored by the Deputy designated safeguarding lead who follows up any incidents following the agreed procedures.
* Any Online safety incident is reported 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. The incident is recorded using the online safety concern proforma and this incident is logged on the online safety incident record held by the Deputy designated safeguarding lead.
* All users will be informed that use of school systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

**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 legislation.
	+ Full information can be found in our GDPR 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**

* We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the: cameras and 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).
* 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.
* 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.

**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 (Jeremy Edwards, Deputy 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, learners and parents.

**7.8.2 Learner email**

* Learners will use provided email accounts for educational purposes.
* Learners 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 and/or Webcams**

* The school does not currently have a bespoke videoconferencing facility and does not participate in use of videoconferencing or webcam use. All staff laptops and school ipads are controlled by the IT manager to ensure that webcams and videoconferencing capabilities are not enabled.
* Should an educational event arise in the future that warrants the use of videoconferencing or webcams then the following policy statements will apply.
* Foreland Fields School recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
	+ All videoconferencing 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.
	+ Videoconferencing contact details will not be posted publically.
	+ Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
	+ Staff will ensure that external videoconferencing 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.

**7.9.1 Users**

* Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
* Learners will ask permission from a member of staff before making or answering a videoconference call or message.
* Videoconferencing will be supervised appropriately, according to the learners 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 videoconferencing administration areas or remote-control pages.
* The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

**7.9.2 Content**

* When recording a videoconference 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 videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

**7.10 Management of Learning Platforms**

* The IT manager, SLT and staff will regularly monitor the usage of the LP (KLZ and purple mash are used currently) by staff and pupils in all areas, in particular message and publishing facilities.
* 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**

* The school uses Tapestry (EYFS), Evidence for Learning and Pupil Asset (Junior, secondary and 6th Form) to track pupils progress and share appropriate information with parents and carers.
* The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and data protection legislation.
* 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.

**8. Social Media**

**8.1 Expectations**

* The expectations’ regarding safe and responsible use of social media applies to all members of Foreland Fields School community.
* The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
* All members of Foreland Fields School community are expected to engage in social media in a positive, safe and responsible manner.
	+ All members of Foreland Fields School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
* We will control learner and staff access to social media whilst using setting provided devices and systems on site.
	+ The use of social media during setting hours for personal use is only permitted at break and lunchtimes within the allocated staffroom, and never in the presence of children.

* + Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
* Concerns regarding the online conduct of any member of Foreland Fields School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

**8.2 Staff Personal Use of Social Media**

* The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
* Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use 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 members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
* Information and content that staff members have access to as part of their employment, including photos and personal information about learners 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 learners and parents and carers*

* All members of staff are advised not to communicate with or add as ‘friends’ any current or past learners 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).
	+ If ongoing contact with learners 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 learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL.
* Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).
* ClassDojo has been put in place as a safe, education based site which enables communication between parents and staff.

**8.3 Learners Personal Use of Social Media**

* Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
* 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 learners under this age.
* Any concerns regarding learners 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.
* Learners 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 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.

**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 learners 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 learners will be moderated possible.
* Parents and carers will be informed of any official social media use with learners; 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 social media acceptable use policy.
	+ 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.
	+ Ensure that they have appropriate consent before sharing images on the official social media channel.
	+ Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
	+ Not engage with any direct or private messaging with current, or past, learners, parents and carers.
	+ Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.
1. **Use of Personal Devices and Mobile Phones**
* Foreland Fields School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

**9.1 Expectations**

* All use of personal devices (including but not limited to; tablets, games consoles and ‘smart’ watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
* Electronic devices of any kind that are brought onto site are the responsibility of the user.
	+ All members of Foreland Fields School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
	+ All members of Foreland Fields School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
* Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
* The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
* All members of Foreland Fields School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

**9.2 Staff Use of Personal Devices and Mobile Phones**

* Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
* Mobile phones may not be used by staff during lessons or allocated school time. They should not be carried by staff (on their person) but should be kept in a locker or secure location away from children. Group leaders accompanying pupils during an off-site activity must ensure they take a phone with them for emergencies and list the number on the journey plans. These phones should only be used in an emergency and, should the leader assist pupils with intimate care needs or be separated from the main group, they should hand them over to another responsible adult.
* Staff will be advised to:
	+ Only use their phones at break and lunchtimes within the allocated staff room. The Bluetooth functionality or other forms of communication (such as ‘airdrop’) of a mobile phone should be switched off at all times and may not be used to send images or files to other mobile phones. Keep mobile phones and personal devices in a locker or safe and secure place. On no account should mobile phones be used in certain areas within the school site such as changing rooms and toilets.
	+ Not use personal devices during teaching periods, unless written permission has been given by the Headteacher or Deputy DSL responsible for Online Safety, such as in emergency circumstances.
	+ Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
* Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
	+ Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy).
* Staff will not use personal devices:
	+ To take photos or videos of learners and will only use work-provided equipment for this purpose.
	+ Directly with learners and will only use work-provided equipment during lessons/educational activities.
* If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
	+ If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

**9.3 Learners Use of Personal Devices and Mobile Phones**

* Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
* Foreland Fields School expects learners’ personal devices and mobile phones to be kept in a secure place, switched off, kept out of sight during lessons and while moving between lessons.
* If a learner needs to contact his/her parents or carers they will be allowed to use a school phone.
	+ Parents are advised to contact their child via the setting office; exceptions may be permitted on a case-by-case basis, as approved by the Headteacher.
* Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of the Headteacher.
	+ The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
	+ If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Headteacher.
* Mobile phones and personal devices must not be taken into examinations.
	+ Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
* If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
	+ Staff may confiscate a learner’s mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
	+ Searches of mobile phone or personal devices will only be carried out in accordance with our policy, which is in line with the DFE Searching, screening and confiscation advice ~~January 2018~~. See[www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))
	+ Learners mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. See [www.gov.uk/government/publications/searching-screening-and-confiscation](http://www.gov.uk/government/publications/searching-screening-and-confiscation))
	+ Mobile phones and devices that have been confiscated will be released to parents or carers at the completion of any investigation.
	+ If there is suspicion that material on a learner’s personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

**9.4 Visitors’ Use of Personal Devices and Mobile Phones**

* Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
* We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
* Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use their mobile phones and personal devices in accordance with our acceptable use of technology policy and other associated policies, including but not limited to anti-bullying, behaviour, child protection and image use.
* Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

**9.5 Officially provided mobile phones and devices**

* Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
* Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
* Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.
1. **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 and illegal content.
* All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
	+ Learners, 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 learners 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 Learners 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.
* All concerns about learners 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, learners can also abuse their peers; all online peer on peer 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 learners 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.

**~~10.2 Staff Misuse~~**

* ~~Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations against school staff policy.~~
* ~~Any allegations regarding a member of staff’s online conduct will be discussed with the LADO (Local Authority Designated Officer).~~
* ~~Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.~~

**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 Headteacherand/or DSL (or deputy).The Headteacherand/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](https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges)” (2018) guidance and part 5 of ‘[Keeping children safe in education’](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2) 2019.
	+ Full details of our response to peer on peer abuse, including sexual violence and harassment can be found in our child protection policy.
* 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
* We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
* If made aware of any concerns relating to online sexual violence and sexual harassment, we will:
	+ immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
	+ if content is contained on learners personal devices, they will be managed in accordance with the DfE ‘[searching screening and confiscation’](https://www.gov.uk/government/publications/searching-screening-and-confiscation) advice.
	+ provide the necessary safeguards and support for all learners involved, such as implementing safety plans, offering advice on blocking, reporting and removing online content, and providing appropriate counselling/pastoral support.
	+ implement appropriate sanctions in accordance with our behaviour policy.
	+ inform parents and carers, if appropriate, about the incident and how it is being managed.
	+ If appropriate, make referrals to partner agencies, such as Children’s Social 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 learners.

**11.2 Youth Produced Sexual Imagery (“Sexting”)**

* Foreland Fields School recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy DSL responsible for online safety).
* We will follow the advice as set out in the non-statutory UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) and [KSCB](http://www.kscb.org.uk/guidance/online-safety) guidance: “Responding to youth produced sexual imagery”.
	+ Youth produced sexual imagery or ‘sexting’ is defined as the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18. It includes nude or nearly nude images and/or sexual acts.
	+ It is an offence to possess, distribute, show and make indecent images of children. The Sexual Offences Act 2003 defines a child, for the purposes of indecent images, as anyone under the age of 18.
* Foreland Fields School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
* We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
* We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
* We will not:
	+ View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
		- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL responsible for online safety) and their justification for viewing the image will be clearly documented.
	+ Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
* If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
	+ Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board’s procedures.
	+ Ensure the DSL (or deputy DSL responsible for online safety) responds in line with the [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) guidance.
	+ Store the device securely.
		- If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
	+ Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
	+ Inform parents and carers, if appropriate, about the incident and how it is being managed.
	+ Make a referral to Children’s Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) guidance.
	+ Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
	+ Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
	+ Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis) guidance.
		- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
	+ Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

**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).
* We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
* We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
* We will ensure that the ‘Click CEOP’ report button is visible and available to learners and other members of our community.
* 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 learners, such as, offering counselling or pastoral support.
	+ Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
* We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
	+ Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: [www.ceop.police.uk/safety-centre/](http://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 learners 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.
	+ Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via [www.iwf.org.uk](https://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](https://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**

* Cyberbullying, along with all other forms of bullying, will not be tolerated at Foreland Fields School.
* Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

**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 andwill be responded to in line with existing policies, including anti-bullying and behaviour.
* All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
* The Police will be contacted if a criminal offence is suspected.
* If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (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 learners 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.
* 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.

**Accidental Exposure**

Report to Internet Watch Foundation ([www.iwf.org.uk](http://www.iwf.org.uk)), the police and/or Front Door, as appropriate

Record incident, action taken and decision making in line with child protection recording systems.

Review policies and procedures and implement changes

**Responding to an Online Safety Concern Flowchart**

**Illegal or Harmful Contact or Conduct**

**Key Local Contacts**

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

**Area Education Safeguarding Advisor:** Name, contact info

**Education Safeguarding Advisor (Online Safety):** 03000 415797

**Front Door:** 03000 411111

**LADO:** 03000 410888

**Police:** 101 or 999 if immediate risk of harm

Consult with Education Safeguarding Service

**Child**

**Online Safety Concern**

Consult with Education Safeguarding Service

**Member of Staff**

This may include CEOP, The Front Door, and/or the police

Report to DSL

Consult with LADO

Report to Headteacher/ Manager in line with allegations policy

If criminal or child protection investigation required

Report to DSL

Report to Internet and/or Filtering Service Provider

**Possible Internal Actions**

* Sanctions (if deliberate)
* PSHE/citizenship
* Restorative justice
* Anti-bullying
* Parental work
* School support e.g. counselling, peer mentoring
* Request support/advice from Education Safeguarding Service

**Conduct**

**Inappropriate Conduct or Content**

**Child**

**Unsure**

**Illegal Content**

**Member of Staff**

Inform the Designated Safeguarding Lead

**Content**

**Possible Internal Actions**

* Staff training
* Disciplinary action if deliberate – if member of staff, contact personnel provider
* Internal support e.g. counselling
* Request support/advice from Education Safeguarding Service

**Deliberate**

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

1. **Useful Links for Educational Settings**

**Kent Educational Setting Support and Guidance**

**Education Safeguarding Service, The Education People**:

* 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](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)
	+ [www.theeducationpeople.org/blog/?tags=Online+Safety&page=1](http://www.theeducationpeople.org/blog/?tags=Online+Safety&page=1)

**KSCMP:** [www.kscb.org.uk](http://www.kscb.org.uk)

**Kent Police:**

* [www.kent.police.uk](http://www.kent.police.uk) or [www.kent.police.uk/internetsafety](http://www.kent.police.uk/internetsafety)
* Inan 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](http://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](http://www.eisit.uk/)

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

* CEOP:
	+ [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)
	+ [www.ceop.police.uk](http://www.ceop.police.uk)
* Internet Watch Foundation (IWF): [www.iwf.org.uk](http://www.iwf.org.uk)
* UK Council for Internet Safety (UKCIS): [www.gov.uk/government/organisations/uk-council-for-internet-safety](https://www.gov.uk/government/organisations/uk-council-for-internet-safety)
* UK Safer Internet Centre: [www.saferinternet.org.uk](http://www.saferinternet.org.uk)
	+ Professional Online Safety Helpline: [www.saferinternet.org.uk/about/helpline](http://www.saferinternet.org.uk/about/helpline)
	+ Report Harmful Content: <https://reportharmfulcontent.com/>
* 360 Safe Self-Review tool for schools: [www.360safe.org.uk](http://www.360safe.org.uk/)
* Childnet: [www.childnet.com](http://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](http://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](http://www.childnet.com/resources/cyberbullying-guidance-for-schools)
* Internet Matters: [www.internetmatters.org](http://www.internetmatters.org)
* Parent Zone: [https://parentzone.org.uk](https://parentzone.org.uk/)
* Parent Info: [https://parentinfo.org](https://parentinfo.org/)
* NSPCC: [www.nspcc.org.uk/onlinesafety](http://www.nspcc.org.uk/onlinesafety)
	+ ChildLine: [www.childline.org.uk](http://www.childline.org.uk)
	+ Net Aware: [www.net-aware.org.uk](http://www.net-aware.org.uk)
* Lucy Faithfull Foundation: [www.lucyfaithfull.org](http://www.lucyfaithfull.org)
* The Marie Collins Foundation: [www.mariecollinsfoundation.org.uk](http://www.mariecollinsfoundation.org.uk/)
* Action Fraud: [www.actionfraud.police.uk](http://www.actionfraud.police.uk/)
* Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org/)