The John Fisher School

E Safety Policy

Responsible: Governors' SLAW Committee

Review Date: September 2023

Aims & Responsibilities

1.1 Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

1.2 Policy scope

- ☐ The John Fisher School believes that online safety (e-Safety) is an essential element of safeguarding students and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles.
- ☐ The John Fisher School identifies that the internet and information communication technologies are an important part of everyday life, so students must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.
- ☐ The John Fisher School has a duty to provide the community with quality Internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.
- ☐ The John Fisher School identifies that there is a clear duty to ensure that all students and staff are protected from potential harm online.
- ☐ The purpose of The John Fisher School online safety policy is to:
    - Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that The John Fisher School is a safe and secure environment.
    - Safeguard and protect all members of The John Fisher School community online.

- Raise awareness with all members of The John Fisher School community regarding the potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

☐ This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff 'in this policy) as well as students and parents/carers.

☐ This policy applies to all access to the internet and use of information communication devices, including personal devices, or where students, staff or other individuals have been provided with school issued devices for use off-site, such as work laptops, tablets or mobile phones.

☐ This policy must be read in conjunction with other relevant school policies including (but not limited to) safeguarding and child protection, anti-bullying, behaviour, confidentiality, confiscation and relevant curriculum policies including ICT and computing, Personal Social and Health Education (PSHE).

1.3 Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

1.4 Writing and reviewing the online safety policy

The Designated Safeguarding Lead (DSL) is **Mr Mawer- Assistant Headteacher.**

E-safety Coordinator is the **Subject Coordinator of ICT**

☐ The John Fisher School online safety policy has been written by the school, involving staff, students and parents/carers, building on the Sutton Safeguarding Children Board's guidance.

- ☐ The policy has been approved and agreed by the Leadership Team and Governing Body**.**
- ☐ The school has appointed the Designated Safeguarding Lead as an appropriate member of the leadership team.
- ☐ The school has appointed Subject Coordinator: ICT responsibility for online safety (e-Safety).
- ☐ The online safety (e–Safety) Policy and its implementation will be reviewed by the school at least annually or sooner if required.

1.5 The key responsibilities of the school management and leadership team are:

- ☐ Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community.
- ☐ Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- ☐ Supporting the Designated Safeguarding Lead (DSL) by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities.
- ☐ Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy which covers appropriate professional conduct and use of technology.
- ☐ To ensure that suitable and appropriate filtering and monitoring systems are in place to protect students from inappropriate content which meet the needs of the school community whilst ensuring students have access to required educational material.
- ☐ To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored.
- ☐ Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications.
- ☐ Ensuring that online safety is embedded within a progressive whole school curriculum which enables all students to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours.
- ☐ To be aware of any online safety incidents and ensure that external agencies and support are liaised with as appropriate.
- ☐ Receiving and regularly reviewing online safeguarding records and using them to inform and shape future practice.
- ☐ Ensuring there are robust reporting channels for the school 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, including ensuring the safe and responsible use of devices.
- ☐ To ensure a member of the Governing Body is identified with a lead responsibility for supporting online safety.
- ☐ Auditing and evaluating current online safety practice to identify strengths and areas for improvement.
- ☐ To ensure that the Designated Safeguarding Lead (DSL) works with the ICT Technicians.

1.6 The key responsibilities of the Designated Safeguarding Lead are:

- ☐ Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate.
- ☐ Keeping up-to-date with current research, legislation and trends regarding online safety.
- ☐ Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day.
- ☐ Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- ☐ Work with the school lead for data protection and data security to ensure that practice is in line with current legislation.
- ☐ Maintaining a record of online safety concerns/incidents and actions taken as part of the schools safeguarding recording structures and mechanisms.
- ☐ Monitor the school's online safety incidents to identify gaps/trends and use this data to update the school's education response to reflect need.
- ☐ To report to the school management team, Governing Body and other agencies as appropriate, on online safety concerns and local data/figures.
- ☐ Liaising with the local authority and other local and national bodies, as appropriate.
- ☐ Working with the school leadership and management to review and update the online safety policies, Acceptable Use Policies (AUPs) and other related policies on a regular basis (at least annually) with stakeholder input.
- ☐ Ensuring that online safety is integrated with other appropriate school policies and procedures.
- ☐ Meet regularly with the governor/board/committee member with a lead responsibility for online safety.

1.7 The key responsibilities for all members of staff are:

- ☐ Contributing to the development of online safety policies.
- ☐ Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- ☐ Taking responsibility for the security of school systems and data.
- ☐ Having an awareness of a range of different online safety issues and how they may relate to the students in their care.
- ☐ Modelling good practice when using new and emerging technologies.
- ☐ Embedding online safety education in curriculum delivery wherever possible.
- ☐ Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures.
- ☐ Knowing when and how to escalate online safety issues, internally and externally.
- ☐ Being able to signpost to appropriate support available for online safety issues, internally and externally.
- ☐ Maintaining a professional level of conduct in their personal use of technology, both on and off site.
- ☐ Demonstrating an emphasis on positive learning opportunities.
- ☐ Taking personal responsibility for professional development in this area.

1.8 In addition to the above, the key responsibilities for staff managing the technical environment are:

- ☐ Providing a safe and secure technical infrastructure which support safe online practices while ensuring that learning opportunities are still maximised.
- ☐ Taking responsibility for the implementation of safe security of systems and data in partnership with the leadership and management team.
- ☐ To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices.
- ☐ Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the DSL.
- ☐ Ensuring that the use of the school's network is regularly monitored and reporting any deliberate or accidental misuse to the DSL.
- ☐ Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- ☐ Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure.
- ☐ Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues.
- ☐ Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- ☐ Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- ☐ Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices.
- ☐ Ensure that appropriately strong passwords are applied and enforced for all users.

1.9 The key responsibilities of children and young people are:

- ☐ Contributing to the development of online safety policies.
- ☐ Reading the school Acceptable Use Policies (AUPs) and adhering to them.
- ☐ Respecting the feelings and rights of others both on and offline.
- ☐ Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues.

At a level that is appropriate to their individual age, ability and vulnerabilities:

- ☐ Taking responsibility for keeping themselves and others safe online.
- ☐ Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- ☐ Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.10 The key responsibilities of parents and carers are:

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

2. Online Communication and Safer Use of Technology

2.1 Managing the school website

- ☐ The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education (DfE).
- ☐ The contact details on the website will be the school address, email and telephone number. Staff or students' personal information will not be published.
- ☐ The Headteacher will take overall editorial responsibility for online content published and will ensure that information is accurate and appropriate.
- ☐ The website will comply with the school's guidelines for publications including accessibility respect for intellectual property rights, privacy policies and copyright.
- ☐ Students work will be published with their permission or that of their parents/carers.
- ☐ The administrator account for the school website will be safeguarded with an appropriately strong password.
- ☐ The school will post information about safeguarding and child protection, including online safety, on the school website for members of the school community, parents/carers and the public.

2.2 Publishing images and videos online

- ☐ The school will ensure that all images and videos shared online are used in accordance with the school image use policy.
- ☐ The school will ensure that all use of images and videos take place in accordance with other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.
- ☐ Written permission from parents or carers will always be obtained before images/videos of students are electronically published.

2.3 Managing email

- ☐ Students may only use school provided email accounts for educational purposes.
- ☐ All members of staff are provided with a specific school email address to use for any official communication.
- ☐ The use of personal email addresses by staff for any official school business is not permitted.
- ☐ The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- ☐ Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email.
- ☐ Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school policies e.g. confidentiality.
- ☐ Members of staff must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records.
- ☐ Staff will be encouraged to develop an appropriate work life balance when responding to email, especially if communication is taking place between staff and students and parents/carers.
- ☐ Excessive social email use can interfere with teaching and learning and will be restricted. Access in school to external personal email accounts may be blocked.
- ☐ Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.
- ☐ The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.
- ☐ School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Official videoconferencing and webcam use for educational purposes

- ☐ The school acknowledges that videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- ☐ All videoconferencing equipment will be switched off when not in use and where appropriate, not set to auto answer.
- ☐ External IP addresses will not be made available to other sites.
- ☐ Videoconferencing contact details will not be posted publically.
- ☐ Video conferencing equipment will be kept securely and, if necessary, locked away when not in use.
- ☐ School videoconferencing equipment will not be taken off school premises without permission.
- ☐ Staff will ensure that external videoconference opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access events are appropriately safe and secure.

Users

- ☐ Students will ask permission from a teacher before making or answering a videoconference call or message.
- ☐ Videoconferencing will be supervised appropriately by members of staff.
- ☐ Parents and carers consent will be obtained prior to children taking part in videoconferencing activities.
- ☐ 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.
- ☐ Unique log on and password details for the educational video conferencing services will only be issued to members of staff and kept secure.

Content

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

2.5 Appropriate and safe classroom use of the internet and any associated devices

- ☐ Internet use is a key feature of educational access and all students will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum *(see specific curriculum policies for further information*).
- ☐ The school's internet access will be designed to enhance and extend education.
- ☐ Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of students.
- ☐ All members of staff are aware that they cannot rely on filtering alone to safeguard students and supervision, classroom management and education about safe and responsible use is essential.
- ☐ During school trips and residentials, the school will decide when it is appropriate for students to use their device and balance students' ability to take part in age appropriate peer activities online with the need for the members of staff to detect abuse, bullying or unsafe practice by students in accordance with the safeguarding and child protection, behaviour, e-safety and all other related policies and procedures.
- ☐ All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- ☐ Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- ☐ Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- ☐ The school will use age appropriate search tools *such as, Google Safe Search or CBBC safe search etc.* as decided by the school following an informed risk assessment to identify which tool best suits the needs of our school community.
- ☐ The school will ensure that the use of Internet-derived materials by staff and students complies with copyright law and acknowledge the source of information.
- ☐ Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- ☐ The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
- ☐ The school will use the internet to enable students and staff to communicate and collaborate in a safe and secure environment.

2.6 Management of school learning platforms / portals / gateways

- ☐ The Leadership Team and staff will regularly monitor the usage of the Learning Platform (LP) in all areas, message and communication tools and publishing facilities.
- ☐ Students/staff will be advised about acceptable conduct and use when using the LP.
- ☐ Only members of the current student, parent/carers 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, students' etc. leave the school their account or rights to specific school areas will be disabled.
- ☐ Any concerns about content on the LP will 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 the Leadership Team before reinstatement.
  e) A student's parent/carer may be informed.
- ☐ A visitor may be invited onto the LP by a member of the Leadership Team. In this instance, there may be an agreed focus or a limited time slot.

3. Social Media

3.1. General social media use

- ☐ Expectations regarding safe and responsible use of social media will apply to all members of The John Fisher School community and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include

blogs, wikis, social networking sites, forums, bulletin boards, apps, video/photo sharing sites, chatrooms, instant messenger and many others.

- ☐ All members of The John Fisher School will be encouraged to engage in social media in a positive, safe and responsible manner at all times.
- ☐ Information about safe and responsible use of social media will be communicated clearly and regularly to all members of staff at The John Fisher School.
- ☐ All members of staff at The John Fisher School 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.
- ☐ The school will control student and staff access to social media and social networking sites whilst on site and when using school provided devices and systems.
- ☐ The use of social networking applications during school hours for personal use **is NOT** permitted.
- ☐ Inappropriate or excessive use of social media during school hours or whilst using school devices by members of staff or students may result in disciplinary action and/or removal of Internet facilities. Where appropriate the police or children and social care will be notified.
- ☐ Any concerns regarding the online conduct of any member of staff at The John Fisher School on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection.
- ☐ Any breaches of school policy may result in disciplinary action being taken and this will depend upon the age of those involved and the circumstances of the breach. Action taken will be in accordance with relevant policies, such as anti-bullying, allegations against staff, behaviour and safeguarding and child protection.

3.2. Official use of social media

- ☐ The John Fisher School official social media channels are: *Twitter, Instagram, LinkedIn, and Facebook.*
- ☐ Official use of social media sites by the school will only take place with clear educational or community engagement objectives with specific intended outcomes e.g. increasing parental engagement.
- ☐ Official use of social media sites as communication tools will be risk assessed and formally approved by the Headteacher.
- ☐ Official school social media channels will be set up as distinct and dedicated social media site or account for educational or engagement purposes.
- ☐ Staff will use school provided email addresses to register for and manage any official approved social media channels.
- ☐ Members of staff running official social media channels will sign a specific Acceptable Use Policy (AUP) to ensure they are aware of the required behaviours and expectations of use and to ensure that sites are used safely, responsibly and in accordance with local and national guidance and legislations.
- ☐ All communication on official social media platforms will be clear, transparent and open to scrutiny.
- ☐ Any online publication on official social media sites will comply with legal requirements including the Data Protection Act 2018, right to privacy conferred by the Human Rights

Act 1998, or similar duty to protect private information and will not breach any common law duty of confidentiality, copyright etc.

- ☐ Official social media use will be in line with existing policies including anti-bullying and child protection.
- ☐ Images or videos of students will only be shared on official social media sites/channels in accordance with school policy and with the agreement of parents and carers.
- ☐ Information about safe and responsible use of social media channels will be communicated clearly and regularly to all members of the community.
- ☐ Official social media sites, blogs or wikis will be suitably protected (e.g. password protected) and where possible/appropriate, run and/or linked to from the school website and take place with written approval from the Leadership Team.
- ☐ Members of the school Leadership team must be aware of account information and relevant details for social media channels in case of emergency, such as staff absence.
- ☐ Public communications on behalf of the school will, where possible, be read and agreed by Senior Leadership.
- ☐ Official social media channels will link back to the school website and/or Acceptable Use Policy to demonstrate that the account is official.
- ☐ The school 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.

3.3 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 the school Acceptable Use Policy.
- ☐ All members of staff are advised not to communicate with or add as 'friends' any current or past students or current or past students' 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 the Designated Safeguarding Lead and/or the Headteacher.
- ☐ If ongoing contact with students is required once they have left the school roll, then members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- ☐ All communication between staff and members of the school community on school business will take place via official approved communication channels.
- ☐ Staff will not use personal social media accounts to contact students or parents/carers, nor should any contact be accepted, except in circumstances whereby prior approval has been given by the Headteacher.
- ☐ Any communication from students or parents/carers received on personal social media accounts will be reported to the schools designated safeguarding lead.
- ☐ Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members, colleagues etc. will not be shared or discussed on personal social media sites.

- ☐ All members of staff are strongly advised to safeguard themselves and their privacy when using social media sites. This will include being aware of location sharing services, setting the privacy levels of their personal sites as strictly as they can, opting out of public listings on social networking sites, logging out of accounts after use and keeping passwords safe and confidential.
- ☐ 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 with school's policies such safeguarding and chid protection, confidentiality, data protection etc. and the wider professional and legal framework.
- ☐ Members of staff will be encouraged to manage and control the content they share and post online. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis.
- ☐ Members of staff will notify the Leadership Team immediately if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school.
- ☐ Members of staff are encouraged not to identify themselves as employees of The John Fisher School on their personal social networking accounts. This is to prevent information on these sites from being linked with the school and also to safeguard the privacy of staff members and the wider community.
- ☐ Members of staff will ensure that they do not represent their personal views as that of the school on social media.
- ☐ School email addresses will not be used for setting up personal social media accounts.
- ☐ Members of staff who follow/like the school's social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.

3.4 Staff official use of social media

- ☐ If members of staff are participating in online activity as part of their capacity as an employee of the school, then they are requested to be professional at all times and to be aware that they are an ambassador for the school.
- ☐ Staff using social media officially will disclose their official role/position but always make it clear that they do not necessarily speak on behalf of the school.
- ☐ Staff using social media officially will be responsible, credible, fair and honest at all times and consider how the information being published could be perceived or shared.
- ☐ Staff using social media officially will always act within the legal frameworks they would adhere to within the workplace, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- ☐ Staff must ensure that any image posted on any official social media channel have appropriate written parental consent.
- ☐ Staff using social media officially will be accountable and must not disclose information, make commitments or engage in activities on behalf of the school unless they are authorised to do so.

- ☐ Staff using social media officially will inform their line manager, the Designated Safeguarding Lead and/or the Headteacher of any concerns such as criticism or inappropriate content posted online.
- ☐ Staff will not engage with any direct or private messaging with students or parents/carers through social media and will communicate via official communication channels.
- ☐ Staff using social media officially will sign the school social media Acceptable Use Policy.

3.5 Students use of social media

- ☐ Safe and responsible use of social media sites will be outlined for students and their parents/carers as part of the Acceptable Use Policy.
- ☐ Personal publishing on social media sites will be taught to students as part of an embedded and progressive education approach via age appropriate sites which have been risk assessed and approved as suitable for educational purposes.
- ☐ Students will be advised to consider the risks of sharing personal details of any kind on social media sites which may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs etc.
- ☐ Students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- ☐ Students will be advised on appropriate security on social media sites and will be encouraged to use safe passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- ☐ Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- ☐ Parents/carers will be informed of any official social media use with students and written parental consent will be obtained, as required.
- ☐ Any official social media activity involving students will be moderated by the school where possible.
- ☐ The school is aware that many popular social media sites state that they are not for students under the age of 13, therefore the School will not create accounts within school specifically for students under this age.
- ☐ Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be dealt with in accordance with existing school policies including anti-bullying and behaviour.
- ☐ Any concerns regarding students' use of social networking, social media and personal publishing sites, both at home and at school, will be raised with parents/carers, particularly when concerning any underage use of social media sites.
- ☐ Further advice for Students & Parents regarding social media can be found via links below.

https://youngminds.org.uk/find-help/for-parents/parents-guide-to-support-a-z/parents-guide-to-support-social-media-and-the-internet/
https://www.net-aware.org.uk/

4. Use of Personal Devices and Mobile Phones

4.1 Rationale regarding personal devices and mobile phones

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

4.2 Expectations for safe use of personal devices and mobile phones

- ☐ All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies.
- ☐ Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- ☐ Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, canteen, play areas and toilets.
- ☐ The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school's behaviour policy.
- ☐ Members of staff will use a work phone number and email address where contact with students or parents/carers is required.
- ☐ All members of The John Fisher School will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- ☐ All members of The John Fisher School will be advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and pin numbers should be kept confidential. Mobile phones and personal devices should not be shared.
- ☐ All members of The John Fisher School will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school's policies.
- ☐ School mobile phones and devices must always be used in accordance with the Acceptable Use Policy and any other relevant policies.
- ☐ School mobile phones and devices used for communication with parents/carer and students must be suitably protected via a passcode/password/pin and must only be accessed and used by members of staff.

4.3 Students use of personal devices and mobile phones

- ☐ Students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- ☐ All use of mobile phones and personal devices by students will take place in accordance with the acceptable use policy.
- ☐ Student's personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during lessons and while moving between lessons.
- ☐ Mobile phones or personal devices will not be used by students during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. 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 students to use their mobile phones or personal devices as part of an educational activity, then it will only take place when approved by the Leadership Team.
- ☐ If a student needs to contact his/her parents/carers they will be allowed to use a school phone out of sight of other students and supervised by a member of staff.
- ☐ Parents/carers are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher.
- ☐ Students should protect their phone numbers by only giving them to trusted friends and family members.
- ☐ Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.
- ☐ Mobile phones and personal devices must not be taken into examinations. Students 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 student's withdrawal from either that examination or all examinations.
- ☐ If a student breaches the school policy, then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- ☐ School staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the school's behaviour or bullying policy or could contain explicit sexual images (sexting). The phone or device may be searched by a member of the Leadership team with the consent of the student or parent/carer and content may be deleted or requested to be deleted, if appropriate. Searches of mobile phone or personal devices will only be carried out in accordance with the school's safeguarding and child protection policy and DFE guidance (https://www.gov.uk/government/publications/searching-screening-and-confiscation)**.**
- ☐ If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, then the device will be handed over to the police for further investigation.

4.4 Staff use of personal devices and mobile phones

- ☐ Members of staff are not permitted to use their own personal phones or devices for contacting students, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with the school's Leadership Team.
- ☐ Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- ☐ Staff will not use any personal devices directly with students and will only use work-provided equipment during lessons/educational activities.
- ☐ Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law e.g. data protection as well as relevant school policies and procedures e.g. confidentiality, data security, Acceptable Use etc.
- ☐ Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.
- ☐ Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.
- ☐ Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.
- ☐ Staff will ensure that any content brought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- ☐ If a member of staff breaches the school policy, then disciplinary action will be taken.
- ☐ 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, then the police may be contacted.
- ☐ Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the school's policy on allegations against members of staff.

4.5 Visitors use of personal devices and mobile phones

- ☐ Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's acceptable use policy.
- ☐ Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the school image use policy.
- ☐ The school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- ☐ Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

5 Reducing online risks

5.1 Reducing online risks.

- ☐ The John Fisher School is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace.

- ☐ Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed.
- ☐ The school will ensure that appropriate filtering and monitoring systems are in place to prevent staff and students from accessing unsuitable or illegal content.
- ☐ The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer or device.
- ☐ The school will audit technology use to establish if the online safety (e–Safety) policy is adequate and that the implementation of the policy is appropriate.
- ☐ Methods to identify, assess and minimise online risks will be reviewed regularly by the school's Leadership Team.

5.2 Internet use throughout the wider school community

- ☐ The school will liaise with local organisations to establish a common approach to online safety.
- ☐ The school will provide an Acceptable Use Policy for any guest/visitor who needs to access the school computer system or internet on site.

5.3 Authorising internet access

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

6 Engagement Approaches

6.1 Engagement and education of children and young people

- ☐ An online safety (e-Safety) curriculum will be established and embedded throughout the whole school, to raise awareness regarding the importance of safe and responsible internet use amongst students.
- ☐ Education about safe and responsible use will precede internet access.
- ☐ As far as possible students input will be sought when writing and developing school online safety policies and practices, including curriculum development and implementation.

- ☐ Students will be supported in reading and understanding the Acceptable Use Policy in a way which suits their age and ability.
- ☐ All users will be informed that network and Internet use will be monitored.
- ☐ Online safety (e-Safety) will be included in the PSHE, ICT and Computing programmes of study, covering both safe school and home use.
- ☐ Online safety (e-Safety) education and training will be included as part of the transition programme for Year 6 into Year 7 and across the Key Stages and where appropriate.
- ☐ Acceptable Use expectations will be included in planners and posted in all rooms with Internet access.
- ☐ Safe and responsible use of the Internet and technology will be reinforced across the curriculum and within the appropriate subject areas.
- ☐ External support will be used to complement and support the school's internal online safety (e-Safety) education approaches.
- ☐ The school will reward positive use of technology by students.
- ☐ The school will implement peer education to develop online safety as appropriate to the needs of the students.

6.2 Engagement and education of children and young people considered to be vulnerable

- ☐ The John Fisher School is aware that some students may be more vulnerable online due to a range of factors.
- ☐ The John Fisher School will ensure that differentiated and ability appropriate online safety (e-Safety) education is given, with input from specialist staff as appropriate (e.g. SENDCO or Inclusion Officer).

6.3 Engagement and education of staff

- ☐ The online safety (e-Safety) policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of our safeguarding responsibilities.
- ☐ Staff will be made aware that our Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential when using school systems and devices.
- ☐ Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff in a variety of ways, on a regular (at least annual) basis.
- ☐ All members of staff will be made aware that their online conduct out of school could have an impact on their role and reputation within school. The school may take disciplinary action and may report the matter to the police if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- ☐ Members of staff with a responsibility for managing filtering systems or monitor ICT use will be supervised by the Leadership Team and will have clear procedures for reporting issues or concerns.

- ☐ The school will highlight useful online tools which staff should use according to the age and ability of the students.

6.4 Engagement and education of parents and carers

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

7. Managing Information Systems

7.1 Managing personal data online

- ☐ Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.
- ☐ Full information regarding the school's approach to data protection and information governance can be found in the school's Data Protection policy.

7.2 Security and Management of Information Systems

Relevant for all settings who facilitate internet access

- ☐ The security of the school information systems and users will be reviewed regularly.
- ☐ Virus protection will be updated regularly.
- ☐ Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems.
- ☐ Portable media may not be used without specific permission followed by an anti-virus /malware scan.
- ☐ Unapproved software will not be allowed in work areas or attached to email.
- ☐ Files held on the school's network will be regularly checked.
- ☐ The network manager will review system capacity regularly.

- ☐ The appropriate use of user logins and passwords to access the school network will be enforced for users.
- ☐ All users will be expected to log off or lock their screens/devices if systems are unattended.
- ☐ The school will log and record internet use on all school owned and private devices.

Password procedures

- ☐ 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 students must always keep their password private and must not share it with others or leave it where others can find it.
- ☐ 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 year *7*, all students are provided with their own unique username and private passwords to access school systems. Students are responsible for keeping their password private.
- ☐ We require staff and students to use STRONG passwords for access into our system.
- ☐ We require staff and students to change their passwords every year.
- ☐ The school's recommendation is that passwords must contain 12 characters including a number and symbol.

7.3 Filtering and Monitoring

- ☐ The governors and Leadership Team will ensure that the school has age and ability appropriate filtering and monitoring in place whilst using school devices and systems to limit student's exposure to online risks.
- ☐ The school's internet access strategy will be dependent on the need and requirements of our school community and will therefore be designed to suit the age and curriculum requirements of our students, with advice from technical, educational and safeguarding staff.
- ☐ All monitoring of school owned/provided systems will take place to safeguard members of the school community.
- ☐ 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.
- ☐ The school uses educational filtered secure broadband connectivity appropriate to the age and requirement of our students.
- ☐ 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 work with Sutton LA, the School's ICT Technician team and filtering /broadband provider to ensure that filtering procedures is continually reviewed.
- ☐ The school will have a clear procedure for reporting breaches of filtering which all members of the school community (all staff and all students) will be made aware of.
- ☐ If staff or students discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and will then be recorded and escalated as appropriate.

- ☐ 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.
- ☐ Any material that the school believes is illegal will be reported to appropriate agencies such as Police or CEOP immediately.

7.4 Management of applications (apps) used to record student's progress:

- ☐ The Headteacher is ultimately responsible for the security of any data or images held of students.
- ☐ Apps/systems which store personal data will be risk assessed prior to use.
- ☐ Only school issued devices will be used to record and store student's personal details, attainment or photographs. Personal staff mobile phones or devices will not be used to access or upload content to any device which record and store student's personal details, attainment or images.
- ☐ Devices will be appropriately encrypted if taken off site to prevent a data security breach in the event of loss or theft.
- ☐ Users will be advised on safety measures to protect all members of the community such as using strong passwords, logging out of systems etc.

8. Responding to Online Incidents and Safeguarding Concerns

- ☐ All members of the community will be made aware of the range of online risks that are likely to be encountered including sexting, online/cyber bullying etc. This will be highlighted within staff training and educational approaches for students.
- ☐ All members of the school community will be informed about the procedure (see Safeguarding & Child Protection policy) for reporting online safety (e-Safety) concerns, such as breaches of filtering, sexting, cyberbullying, illegal content etc.
- ☐ The Designated Safeguarding Lead (DSL) will be informed of any online safety (e-Safety) incidents involving child protection concerns, which will then be recorded.
- ☐ The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Sutton Safeguarding Children Board thresholds and procedures.
- ☐ Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- ☐ Complaints about online/cyber bullying will be dealt with under the School's anti-bullying policy and procedure
- ☐ Any complaint about staff misuse will be referred to the Headteacher

- ☐ Any allegations against a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- ☐ Students, parents and staff will be informed of the schools complaints procedure.
- ☐ Staff will be informed of the complaints and whistleblowing procedure.
- ☐ All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns.
- ☐ All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.
- ☐ The school will manage online safety (e-Safety) incidents in accordance with the school discipline/behaviour policy where appropriate.
- ☐ The school will inform parents/carers of any incidents of concerns as and when required.
- ☐ After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes as required.
- ☐ Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Education Safeguards Team or Police via 101 or 999 if there is immediate danger or risk of harm.
- ☐ The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the Police.
- ☐ If the school is unsure how to proceed with any incidents of concern, then the incident will be escalated to the Education Safeguarding Team.
- ☐ If an incident of concern needs to be passed beyond the school community, then the concern will be escalated to the Education Safeguarding Team to communicate to other schools/settings in Sutton.
- ☐ Parents/carers and students will need to work in partnership with the school to resolve issues.

Appendix A

9. Procedures for Responding to Specific Online Incidents or Concerns

9.1 Responding to concerns regarding Youth Produced Sexual Imagery or "Sexting"

- ☐ The John Fisher School will ensure that all members of staff are made aware of the potential social, psychological and criminal consequences of sharing, possessing and creating youth produced sexual imagery (known as "sexting").
- ☐ The school will implement preventative measures for students, staff and parents/carers.
- ☐ The John Fisher School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- ☐ The school will follow the guidance as set out in our safeguarding and child protection policy, the advice on 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and Sutton Safeguarding Board guidance.
- ☐ If the school are made aware of incidents involving creating youth produced sexual imagery the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Children Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store the device securely.
    - Carry out a risk assessment in relation to the students(s) involved.
    - Consider the vulnerabilities of students(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to children's social care and/or the police (as needed/appropriate).
    - Put the necessary safeguards in place for students e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Implement appropriate sanctions in accordance with the schools behaviour policy but taking care not to further traumatise victims where possible.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the leadership team will review and update any management procedures where necessary.
    - Inform parents/carers about the incident and how it is being managed.

- ☐ The school will not view any sexual images (suspected of being produced by a student) unless there is no other possible option or there is a clear need or reason to do so (in these cases the image will only be viewed by the Designated Safeguarding Lead).
- ☐ The school will not send, share or save content suspected to be an indecent image of students and will not allow or request students to do so.
- ☐ If an indecent image has been taken or shared on the school network or devices, then the school will take action to block access to all users and isolate the image.

- ☐ The school will take action regarding creating youth produced sexual imagery, regardless of the use of school equipment or personal equipment, both on and off the premises.
- ☐ The school will ensure that all members of staff are aware of sources of support regarding youth produced sexual imagery.

9.2. Responding to concerns regarding Online Child Sexual Abuse and Exploitation

- ☐ The John Fisher School will ensure that all members of the community are made aware of online child sexual abuse, including exploitation and grooming including the consequences, possible approaches which may be employed by offenders to target students and how to respond to concerns.
- ☐ The school will implement preventative approaches for online child sexual abuse via a range of age and ability appropriate educational approaches for students, staff and parents/carers.
- ☐ The John Fisher School views online child sexual abuse as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead
- ☐ If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the Police.
- ☐ If the school is made aware of intelligence or information which may relate to child sexual exploitation (on or offline) then it will be passed through to the CSET team by the DSL.
- ☐ If the school are made aware of an incident involving online child sexual abuse of a child then the school will:
    - Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Children Boards procedures.
    - Immediately notify the designated safeguarding lead.
    - Store any devices involved securely.
    - Immediately inform the police via 101 (using 999 if a child is at immediate risk).
    - Where appropriate the school will involve and empower students to report concerns regarding online child sexual abuse e.g. using the Click CEOP report form: www.ceop.police.uk/safety-centre/
    - Carry out a risk assessment which considers any vulnerabilities of student(s) involved (including carrying out relevant checks with other agencies).
    - Make a referral to student's social care (if needed/appropriate).
    - Put the necessary safeguards in place for student(s) e.g. offer counselling support and immediate protection and offer appropriate pastoral support for those involved.
    - Inform parents/carers about the incident and how it is being managed.
    - Review the handling of any incidents to ensure that the school is implementing best practice and the school leadership team will review and update any management procedures where necessary.
- ☐ The school will take action regarding online child sexual abuse regardless of the use of school equipment or personal equipment, both on and off the school premises.
- ☐ The school will ensure that all members of the community are aware of sources of support regarding online child sexual abuse.

- ☐ If students at other schools are believed to have been targeted, then the school will seek support from the Education Safeguarding Team to enable other schools to take appropriate action to safeguarding their community.
- ☐ The school will ensure that the Click CEOP report button is visible and available to students and other members of the school community, for example including the CEOP report button the school website homepage and on intranet systems.

9.3. Responding to concerns regarding Indecent Images of Children (IIOC)

- ☐ The John Fisher School will ensure that all members of the community are made aware of the criminal nature of Indecent Images of Children (IIOC) including the possible consequences.
- ☐ The school will take action regarding Indecent Images of Children (IIOC) regardless of the use of school equipment or personal equipment, both on and off the premises.
- ☐ The school will take action to prevent accidental access to Indecent Images of Children (IIOC) for example using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list, implementing appropriate web filtering, implementing firewalls and anti-spam software.
- ☐ If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the police.

- ☐ If the school is made aware of Indecent Images of Children (IIOC) then the school will:
  - Act in accordance with the school's child protection and safeguarding policy and the relevant Local Safeguarding Children Boards procedures.
  - Immediately notify the school Designated Safeguard Lead.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations e.g. the Internet Watch Foundation (IWF), the police via 101 (using 999 if a child is at immediate risk) and/or the LADO (if there is an allegation against a member of staff).
- ☐ If the school are made aware that a member of staff or a student has been inadvertently exposed to indecent images of children whilst using the internet, then the school will:
  - Ensure that the Designated Safeguard Lead 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.
- ☐ If the school are made aware that indecent images of children have been found on the schools electronic devices then the school will:
  - Ensure that the Designated Safeguard Lead 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 services (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.

- ☐ If the school are made aware that a member of staff is found in possession of indecent images of students on their electronic device provided by the school, then the school will:
    - Ensure that the Designated Safeguard Lead is informed or another member of staff in accordance with the school whistleblowing procedure.
    - Contact the police regarding the images and quarantine any devices involved until police advice has been sought.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with the schools managing allegations policy.
    - Follow the appropriate school policies regarding conduct.

9.4. Responding to concerns regarding radicalisation and extremism online

- ☐ The school will take all reasonable precautions to ensure that students are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of students.
- ☐ When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- ☐ Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including anti-bullying, behaviour etc. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately via the Education Safeguarding Team and/or the police.

9.5. *Responding to concerns regarding cyberbullying*

- ☐ Cyberbullying, along with all other forms of bullying, of any student or member of staff at The John Fisher School will not be tolerated. Full details are set out in the school policies regarding anti-bullying and behaviour.
- ☐ All incidents of online bullying reported will be recorded.
- ☐ There are clear procedures in place to investigate incidents or allegations and support anyone in the school community affected by online bullying.
- ☐ If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the police.
- ☐ Students, staff and parents/carers will be advised to keep a record of cyberbullying as evidence.
- ☐ The school will take steps to identify the bully where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- ☐ Students, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the schools e-Safety ethos.
- ☐ Consequences for those involved in online or cyberbullying may include:
    - Those involved will be asked to remove any material deemed to be inappropriate or offensive.

- A service provider may be contacted to remove content if those involved refuse to or are unable to delete content.
- Internet access may be suspended at school for the user for a period of time. Other sanctions for students and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy.
- Parent/carers of students involved in online bullying will be informed.
- The Police will be contacted if a criminal offence is suspected.

9.6. *Responding to concerns regarding online hate*

- ☐ Online hate at The John Fisher School will not be tolerated. Further details are set out in the school policies regarding anti-bullying and behaviour and discipline.
- ☐ All incidents of online hate reported to the school will be recorded.
- ☐ All members of the community will be advised to report online hate in accordance with relevant school policies and procedures e.g. anti-bullying, behaviour etc.
- ☐ The Police will be contacted if a criminal offence is suspected. If the school is unclear if a criminal offence has been committed, then the Designated Safeguarding Lead will obtain advice immediately through the Education Safeguarding Team and/or the police.

Appendix B

Online Safety (e-Safety) Contacts and References

Sutton Support and Guidance

Local Safeguarding Children partnership (LSCp): https://www.suttonlscp.org.uk/lscp-esafety.php

Sutton Support for Education Settings

Hayley Cameron: Education Safeguarding Manager hayley.cameron@cognus.org.uk

Stephen Welding: e-Safety Development Officer stephen.welding@cognus.org.uk

Abu Ullah: Prevent and Hate Crime Officer abu.ullah@sutton.gov.uk

The police:
www.sutton.police.uk
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact the police via 101

National Links and Resources

Action Fraud: www.actionfraud.police.uk

BBC WebWise: www.bbc.co.uk/webwise

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

ChildLine: www.childline.org.uk

Childnet: www.childnet.com

Get Safe Online: www.getsafeonline.org

Internet Matters: www.internetmatters.org

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

Lucy Faithfull Foundation: www.lucyfaithfull.org

Know the Net: www.knowthenet.org.uk

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

NSPCC: www.nspcc.org.uk/onlinesafety

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

Report Harmful Content: https://reportharmfulcontent.com

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

Think U Know: www.thinkuknow.co.uk

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

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

Appendix C

Online Safety Incident: If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.