



Online Safety Policy Template for Educational Settings

September 2018

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 Staff Misuse	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

Using the Online Safety Policy Template

An Online safety policy provides educational settings with a framework to develop their online safety ethos and enables leaders and managers to detail strategic approaches and considerations, with regards to the safer use of technology.

The online safety policy should be recognised as a safeguarding policy, not a technical or computing policy and falls within the role and responsibilities the Designated Safeguarding Lead (DSL).

There is no requirement for educational settings to have a separate online safety policy if online safety issues are appropriately addressed within other policies; this decision will be down to leaders and managers. If online safety is embedded within existing documents, settings should ensure that their community is aware of how and where to locate safety information, especially regarding responding to and reporting specific online safety concerns.

We encourage all educational settings to ensure that their online safety policy is individualised for their own specific context, to ensure that it is fit for purpose. It will not be appropriate for educational settings to adopt this template in its entirety; some statements will be more relevant to some settings than others.

This policy template requires leaders, managers and DSLs to adapt the content to include specific local information such as their own named points of contact, as well as their specific procedures and expectations. These decisions and details will vary from setting to setting, so this template should be used as a starting framework.

Disclaimer

The template has been created by the Education People on behalf of East Sussex County Council. 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.

The Oak Tree Federation

Online Safety Policy



Firle Church of England
Primary School

Key Details

Designated Safeguarding Leads: Vicki Brown-Head of School and Rachel West Executive Head Teacher

Named Governor with lead responsibility: Denise Kong and Gemma Collins

Date written: February 2019

Date agreed and ratified by Governing Body: March 2019

Date of next review: March 2020

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

The Oak Tree Federation Online Safety Policy

1. Policy Aims

- This online safety policy has been written by The Oak Tree Federation involving staff, learners and parents/carers, building on the East Sussex 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](#)” 2018, [Early Years and Foundation Stage](#) 2017 and the East Sussex Safeguarding Children Board procedures.
- The purpose of The Oak Tree Federation’s online safety policy is to:
 - Safeguard and protect all members of The Oak Tree Federation’s 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.
- The Oak Tree Federation 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.

2. Policy Scope

- The Oak Tree Federation 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.
- The Oak Tree Federation identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- The Oak Tree Federation 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, 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 Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE),
- Data security
- Privacy notice
- Social Media policy Searching, screening and confiscation policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly; The Oak Tree Federation 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 head teacher will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Vicki Brown, Head of School and Rachel West, Executive Head teacher, have lead responsibility for online safety.
 - Whilst activities of the designated safeguarding lead may be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection remains with the DSL.
- The Oak Tree Federation 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:

- 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/behaviour 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 Designated Safeguarding Lead (DSL) 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.
- Work alongside 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 online safety training.
- 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
- 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 leadership 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, 3 times a year, with the governor with a lead responsibility for safeguarding and online safety.

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.
- 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 such as specific password policies 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.
- Report any filtering breaches to the DSL (or deputy DSLs) and leadership team, as well as, the settings Internet Service Provider or other services, as appropriate.
- Ensure that any safeguarding concerns, identified through monitoring or filtering breaches are reported to the DSL (or deputy DSLs), in accordance with the safeguarding procedures.

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.

5. Education and Engagement Approaches

5.1 Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in Personal, Social, Health and Economic (PSHE) and computing programmes of study.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The setting will support learners to read and understand the 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.
 - Rewarding positive use of technology.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.

- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

5.2 Vulnerable Learners

- The Oak Tree Federation 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.
- The Oak Tree Federation will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners
- When implementing an appropriate online safety policy and curriculum The Oak Tree Federation will seek input from specialist staff as appropriate, including the SENCO (Sophie Levey and Liz Fitzpatrick) and Child in Care Designated Teacher (Vicki Brown/Lynn Filtress)

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.
 - *Online safety training will be delivered alongside existing safeguarding and child protection training which will take place annually. Updates will be included termly into a staff meeting agenda and support staff briefings.*
 - 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

- The Oak Tree Federation 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.

6. Reducing Online Risks

- The Oak Tree Federation recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
 - Regularly review the methods used to identify, assess and minimise online risks.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. Safer Use of Technology

7.1 Classroom Use

- The Oak Tree Federation uses a wide range of technology. This includes access to:
 - Computers, laptops, Ipads and other digital devices
 - Internet which may include search engines and educational websites
 - Email
 - Games consoles and other games-based technologies
 - Digital cameras, web cams and video cameras
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

- 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 learners will be appropriate to their age and ability.
 - **Early Years Foundation Stage and Key Stage 1**
 - 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 learners' age and ability.
 - **Key Stage 2**
 - Learners will use age-appropriate search engines and online tools.
 - Learners 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

- Schools in England and Wales are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" Furthermore, it expects that they "assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. Children should not be able to access harmful or inappropriate material from the school or colleges IT system; however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding." Smoothwall is installed on all devices used in school to ensure we have effective filtering systems in place. The filtering system is reviewed regularly and member of the SLT have access to the online monitoring reports, which are checked regularly.

7.3.1 Decision Making

- The Oak Tree Federation governors and leadership team 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 leadership 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 Filtering

- Education broadband connectivity is provided through East Sussex County Council.
- We use Smoothwall, provided by Schools ICT, which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- We work with Schools ICT and Smoothwall to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
 - turn off the screen or close the laptop 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 deputies) or office 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, Sussex Police or CEOP.

7.3.4 Monitoring

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
 - Physical monitoring in school- (staff supervision),
 - Monitoring internet and web access (reviewing log file information) and/or active/pro-active technology monitoring services.
- If a concern is identified via monitoring approaches we will:
 - Ensure DSL or deputies will respond in line with the child protection policy.
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

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 information security policy on our website.

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.

- Encryption for personal data sent over the Internet 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.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
 - Specific user logins and passwords will be enforced for all year group but these will not be for individual pupils.
- All users are expected to log off or lock their screens/devices if systems are unattended.
- Further information about technical environment safety and security can be found at:
 - Acceptable use policy
 - Code of Conduct
 - Computing Policy
 - Social Media Policy

7.5.1 Password policy

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords to the email every month as required
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

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 policies, 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.

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 inform Mrs Rachel West, Headteacher, or Mrs Vicki Brown, Head of School, 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;
- We will have a dedicated email for reporting safeguarding issues and this will be monitored by the DSLs, deputy DSL and office manager.

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.

7.9 Management of Learning Platforms

- The Oak Tree Federation uses e-Schools website as its official learning platform at Laughton and Firle is run by Union Jack a private provider.
- Leaders and staff will regularly monitor the usage of any Learning Platform (LP), including message/communication tools and publishing facilities (this is currently not available at Firle).
- Only current members of staff, learners and parents will have access to the LP.
- When staff and/or learners leave the setting, their account will be disabled or transferred to their new establishment.
- Learners and staff will be advised about acceptable conduct and use when using the LP.
- All users will be mindful of copyright and will only upload appropriate content onto the LP.
- Any concerns about content on the LP will be recorded and dealt with in the following ways:

- The user will be asked to remove any material deemed to be inappropriate or offensive.
- If the user does not comply, the material will be removed by the site administrator.
- Access to the LP for the user may be suspended.
- The user will need to discuss the issues with a member of leadership before reinstatement.
- A learner's parents/carers may be informed.
- If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- 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.

8. Social Media

8.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of the The Oak Tree Federation 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 the The Oak Tree Federation community are expected to engage in social media in a positive, safe and responsible manner.
 - All members of the The Oak Tree Federation 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 not permitted.
 - 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 the The Oak Tree Federation community on social media should be reported to the DSL (or deputy) 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 The Oak Tree Federation or their individual schools 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 (or deputies) and Mrs West, headteacher. 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 headteacher.

- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputies).

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. .

9. Use of Personal Devices and Mobile Phones

- The Oak Tree Federation recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

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, child protection and the code of conduct.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - All members of The Oak Tree Federation 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 The Oak Tree Federation 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 any changing rooms and toilets. 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 The Oak Tree Federation 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, acceptable use, social media and code of conduct.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson times, teaching times and when on playground duty or at any times when working with children.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times, teaching times and when on playground duty or at any times when working with children.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless written permission has been given by the headteacher such as in emergency circumstances.
 - Ensure that any content brought 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 pupils or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputies) or headteacher.
- 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 or 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.
- The Oak Tree Federation expects learners' personal devices and mobile phones to be...
 - Given in to the office first thing in the morning, if they are brought into school, and collected at the end of the day.
- If a learner needs to contact his/her parents or carers they will be allowed to use the office phone.
 - Parents are advised to contact their child via the setting office

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.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputies) or headteacher of any breaches our policy.

9.5 Officially provided mobile phones and devices

- Members of staff will be issued with an 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.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying 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.
- Safeguarding concerns and incidents should be reported to Single Point of Access, in line with East Sussex Safeguarding and Child Protection model policy.

- If we are unsure how to proceed with an incident or concern, the DSL (or deputies) will seek advice from the Standards and Learning Effectiveness Service Safeguarding Team.
- Where there is suspicion that illegal activity has taken place, we will contact the Standards and Learning Effectiveness Service or Sussex Police using 101, or 999 if there is immediate danger or risk of harm.
- If an incident or concern needs to be passed beyond our community (for example if other local settings are involved or the public may be at risk), the DSL or headteacher will speak with Sussex Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

10.1 Concerns about Learners Welfare

- The DSL (or deputies) will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL (or deputies) will record these issues in line with our child protection policy.
- The DSL (or deputies) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the East Sussex Safeguarding Children Board thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

10.2 Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the allegations 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.

11. Procedures for Responding to Specific Online Incidents or Concerns

11.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "[Sexual violence and sexual harassment between children in schools and colleges](#)" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- The Oak Tree Federation 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, unwanted sexual comments and messages on social media, and online sexual exploitation.

- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- The Oak Tree Federation 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.
- The Oak Tree Federation also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Oak Tree Federation 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 between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and online safety curriculum. (We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- 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 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 learner's electronic devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as 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 a referral to partner agencies, such as Children's Social Care and/or the Police.
 - If the concern involves children and young people at a different educational setting, 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 Sussex 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.

11.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- The Oak Tree Federation 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.

- The Oak Tree Federation recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community.
- 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 East Sussex Safeguarding Child Board's procedures.
 - If appropriate, store any devices involved securely.
 - Make a referral to Children's Social Care (if required/ appropriate) and immediately inform the police via 101 (or 999 if a child is at immediate risk)
 - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.
 - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Standards and Learning Effectiveness Service and/or Police.
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from the Police and/or the Standards and Learning Effectiveness Service first to ensure that potential investigations are not compromised.

11.4 Indecent Images of Children (IIOC)

- The Oak Tree Federation 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) will obtain advice immediately through the Police and/or the Standards and Learning Effectiveness Service.
- If made aware of IIOC, we will:
 - Act in accordance with our child protection policy and the relevant East Sussex Safeguarding Child Boards procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Sussex 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) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
 - Ensure that the DSL (or deputy DSL) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk.
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Inform the police via 101 (999 if there is an immediate risk of harm) and children's social 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.
 - 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 The Oak Tree Federation.
- 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 The Oak Tree Federation and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy DSL) will obtain advice through the Standards and Learning Effectiveness Service and/or Sussex 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.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy DSL) 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.

12. Useful Links for Educational Settings

East Sussex Support and Guidance:

- East Sussex County Council Early Years Support & Intervention Team
 - Call: 01323 463026
 - Email: childcare.support@eastsussex.gov.uk
- If you are concerned about a child in East Sussex contact SPOA (Single Point of Advice) on 01323 464222 or 0-19.SPOA@eastsussex.gov.uk
- Standards and Learning Effectiveness Service (SLES):
SLES.Safeguarding@eastsussex.gov.uk
Support and Intervention Manager: Safeguarding: Dion Page-Hammond
Dion.Page-Hammond@eastsussex.gov.uk
- East Sussex Schools ICT Service: Richard May
Richard.May@eastsussex.gov.uk
- Local Authority Designated Officer: Amanda Glover
Amanda.Glover@eastsussex.gov.uk
- East Sussex Safeguarding Children Board (LSCB): 01273 481544 or
lscbcontact@eastsussex.gov.uk

East Sussex Support and Guidance for Educational Settings

- <https://czone.eastsussex.gov.uk/safeguarding/>
- <https://czone.eastsussex.gov.uk/safeguarding/support-for-safeguarding-in-colleges-schools-and-early-years-settings/>

East Sussex Safeguarding Children's Board

- www.sussexchildprotection.procedures.org.uk/

Sussex Police:

www.sussex.police.uk

For non-urgent Police contact 101 or 01273 470101

If you think the child is in immediate danger, you should call the police on 999.

National Links and Resources for Educational Settings

- CEOP:
 - www.thinkuknow.co.uk

- www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/online-safety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.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
- NSPCC: www.nspcc.org.uk/online-safety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk