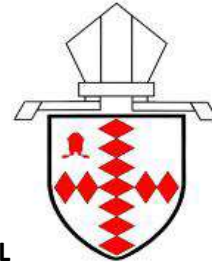




NUTFIELD CHURCH (C OF E) PRIMARY SCHOOL



Online Safety and Acceptable Use Policy

Vision

We fully embrace the vision stated in the Church of England's Vision for Education 'Deeply Christian Serving the Common Good' published in July 2016 of educating the whole person. We aim for our children and members of the wider school community to flourish in all they do and 'live life in all its fullness'. (John 10:10)

Values

- We are a church school, which believes in the importance of **community**, where people from all races, religions and cultures act in **peace** together.
- Our pupils, staff and families work together as a team, with **wisdom** supporting each other through our learning. We have **hope** in our challenges and in our successes.
- We recognise the **dignity** and ultimate worth of each person, created in the image of God, further shaped by the person, teaching and example of Jesus. We look to the future with **joy**.

Reviewed: Summer 2024

Next Review: Summer 2025

1. Aims

Nutfield Church (C of E) Primary 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

- This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, also the Statutory Framework for the Early Years and Foundation Stage 2017 and 'Working Together to Safeguard Children' 2018.
- It takes into account DfE non-statutory advice for schools on:
 - Teaching online safety in schools
 - Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
 - It also refers to the Department'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.
- The policy also takes into account the National Curriculum computing programmes of study.

3. Purpose

- The purpose of Nutfield Church (C of E) Primary School online safety policy is to:
 - Safeguard and protect all members of Nutfield Church (C of E) Primary School community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work and to be able 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.
- Nutfield Church (C of E) Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
 - **Content:** being exposed to illegal, inappropriate or harmful material
 - **Contact:** being subjected to harmful online interaction with other users
 - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

4. Policy Scope

- Nutfield Church (C of E) Primary School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- Nutfield Church (C of E) Primary School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Nutfield Church (C of E) Primary School believes that pupils should be empowered to build digital resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, senior leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy) as well as pupils, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals are accessing the school network remotely.

5. Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying Policy
- Behaviour Policy
- Safeguarding (Child Protection) Policy and Procedures
- Staff Code of Conduct (Staff Behaviour Policy)
- Staff Disciplinary and Capability Policy and Procedures
- Complaints Procedure
- Curriculum policies, such as: Relationships and Sex Education (RSE) and Health Education Policy and Quality of Education Policy
- Data Protection Policy and Privacy Notices

6. Monitoring and Review

- Technology in this area evolves and changes rapidly. Nutfield Church (C of E) Primary School will review this policy at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher 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.

7. Roles and Responsibilities

Nutfield Church (C of E) Primary School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

7.1 The Headteacher:

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. In her role as The Designated Safeguarding Lead (DSL) alongside the senior leadership team and Governors are now integral to the implementation of online safety and carry ultimate responsibility for its delivery. Governing bodies are now required to approve and review the effectiveness of online safety policies and practise

7.2 The Governing Body:

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation. Governors 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 Policy, ICT Acceptable Use Policy – Staff Governors and Volunteers (Appendix 1), Use of Mobile Phones in School Policy (Appendix 2), ICT Acceptable Use Policy – Pupils (Appendix 3), Key Stage One Online Safety Charter (Appendix 4), Key Stage Two Online Safety Charter – in line with Google – Be Internet Awesome (Appendix 5), Nutfield Church Peace Makers’ Charter (Appendix 6), Responding to an Online Safety Concern (Appendix 7) which covers acceptable use of technology in school and Consent form for taking and using photos (Appendix 8).
- 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 pupils to develop an age-appropriate understanding of online safety.
- Support the DSL and deputy DSLs 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. These can be found on the online safety section of the school website:
 - <https://reportharmfulcontent.com/?lang=en>
 - <https://www.ceop.police.uk/safety-centre/>.

7.3 The Designated Safeguarding Lead (DSL):

The Designated Safeguarding Lead (DSL) is: Imogen Woods

The Deputy DSLs are:

- Katharine Brooks
- Anna Benjamin
- Daniel Walker-Cheetham
- Serena Fowler

The DSL takes lead responsibility for online safety in school, in particular:

- 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 pupils 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 DSL Team.
- Work with the Senior Leadership Team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly every half term with the governor with a lead responsibility for safeguarding including online safety.

7.4 All members of staff and volunteers:

- 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.

7.5 Staff managing the technical environment:

- Provide technical support and perspective to the DSL and senior leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Liaise with the Network Provider (JSPC) to implement appropriate security measures as directed by the leadership team to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Liaise with the Network Provider (JSPC) to ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the senior leadership team.
- Liaise with the Network Provider (JSPC) to ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the senior leadership team

7.6 Pupils (at a level that is appropriate to their individual age and ability):

- 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.

7.7 Parents and carers:

- 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.
- Ensure their child has read, understood and agreed to the terms of acceptable use of the school's ICT systems and internet (Appendix 3)
- Role model safe and appropriate use of technology and social media.
- Abide by the equivalent of the Nutfield Church Peace Makers' Charter (Appendix 6)
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from Nutfield Church (C of E) Primary School or the link on the school website, if they or their child encounter risk or concerns online.
- Use our systems, including online subscription sites such as MyMaths.co.uk, and discoveryeducation.co.uk (espresso), and Purple Mash safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

8. Education and Engagement Approaches

8.1 Education and engagement with pupils

Pupils will be taught about online safety as part of the curriculum. They will be taught to use technology safely and respectfully and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in Relationships and Sex Education (RSE) and Health Education and computing programmes of study.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support pupils to read and understand the acceptable use policies in a way which suits their age and ability by:
 - Displaying The Nutfield Church Peace Makers' Charter (Appendix 6)
 - Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.
 - The Class Teachers discussing the Acceptable Use Agreement for Pupils with their class to ensure they understand their behaviour and online use must be in line with the acceptable use agreement (see Appendix 3) and Key Stage One Online Safety Charter (Appendix 4) or Key Stage 2 Online Safety Charter (Appendix 5).

- By the end of primary school, pupils will know:
 - That people sometimes behave differently online, including by pretending to be someone they are not.
 - That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
 - The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
 - How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
 - How information and data is shared and used online
 - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

8.2 Vulnerable Pupils

- Nutfield Church (C of E) Primary School recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Nutfield Church (C of E) Primary School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- When implementing an appropriate online safety policy and curriculum Nutfield Church (C of E) Primary School will seek input from specialist staff as appropriate, including the SENCO and Designated Teacher for Looked-After and Post Looked-After Children.

8.3 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.
- 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.

8.4 Awareness and engagement with parents and carers

- Nutfield Church (C of E) Primary School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats.
 - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
 - Drawing their attention to the online safety policy and expectations in newsletters, letters, 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.

9. Reducing Online Risks

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

10. Safer Use of Technology

10.1 Classroom Use

- Nutfield Church (C of E) Primary School uses a wide range of technology. This includes access to:
 - Laptops and Tablets
 - Internet which may include search engines and educational websites
 - Access to MyMaths.co.uk, and discoveryeducation.co.uk (espresso).
 - 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.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.
- Supervision of pupils will be appropriate to their age and ability.
- **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 pupil's age and ability.
- **Key Stage 2**
 - Pupils will use age-appropriate search engines and online tools.
 - Pupils will be directed by the teacher to online materials and resources which support the learning outcomes planned for the pupil's age and ability.

10.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff and visitors will read and sign an ICT Security Acceptable Use (Appendix 1) and all pupils will sign a Pupil Acceptable Use Agreement (Appendix 3) before being given access to our computer system, IT resources or internet.

10.3 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 Data Protection Policy and Records Management Policy.

10.4 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 pupils' personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

10.5 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the photo permission data gathered at entry to Nutfield Church (C of E) Primary School (Appendix 8 - Consent Form for taking and using photos).

10.6 Managing Email

- Access to our staff email systems will always take place in accordance with data protection legislation and in line with other policies, including safeguarding, 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.
 - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the Headteacher 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.

10.7 Filtering and Monitoring

- We will take all reasonable precautions to ensure that pupils and staff are safe from harmful material when accessing the internet on site. Nutfield Church Primary School's contract with JSPC includes Lightspeed

Systems filtering included with the Broadband package providing fully compliant web filtering based on a comprehensive education-specific database.

- The Lightspeed Systems Web Filter gives real time visibility of all activity on our school's network, provides notifications alerting teachers to suspicious search queries and enables temporary block categories at user, IP, group or domain level and fixed and mobile devices. Its reporting function is compliant with the Prevent Duty to prevent people from being drawn into terrorism.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or a deputy DSL) will be informed immediately, and action will be taken in line with this policy.

11. Social Media

11.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of Nutfield Church (C of E) Primary School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of Nutfield Church (C of E) Primary School community are expected to engage in social media in a positive, safe and responsible manner.
- All members of Nutfield Church (C of E) Primary School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Access to social media in school on personal devices is allowed exclusively in the staffroom or office areas of the school.
- Inappropriate or excessive use of social media at school may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of Nutfield Church (C of E) Primary School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and safeguarding (child protection) policies.

11.2 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 and 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 Nutfield Church (C of E) Primary School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Senior 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 pupils or their family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or a deputy DSL).
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted.
- Any inappropriate communication from pupils and parents received on personal social media accounts will be reported to the DSL (or a deputy DSL).

11.3 Pupils Personal Use of Social Media

- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for pupils under this age.
- However, we are aware that many of our Key Stage 2 children have social media accounts and, as such, the following will apply:
 - Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
 - Any concerns regarding pupils’ use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
 - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- In cases where staff are made aware of the social media accounts of Key Stage 2 children, staff may consider the following bullet points:
 - 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.

12. Use of Personal Devices and Mobile Phones

- Nutfield Church (C of E) Primary School 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.

12.1 Expectations for Staff

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and safeguarding (child protection).
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
- All members of Nutfield Church (C of E) Primary School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
- All members of Nutfield Church (C of E) Primary School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used outside the staffroom and office areas of the school.
- 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 Nutfield Church (C of E) Primary School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or safeguarding (child protection) policies.

12.2 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, safeguarding (child protection), data security and acceptable use.
- Staff will be required to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - 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 bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.

- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers, any pre-existing relationships, which could undermine this, will be discussed with the DSL (or a deputy DSL).
- Staff will not use personal devices:
 - To take photos or videos of pupils and will only use work-provided equipment for this purpose.
 - Directly with pupils and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

12.3 Learners Use of Personal Devices and Mobile Phones

- Children will hand any mobile devices that they bring into school to the office. They can collect them at home time.
- Pupils' mobile devices may not be used at any time on school premises.
- If pupils use their mobile device in school, it will be confiscated and any photographs or other content created during school time will be deleted. School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.
- Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

12.4 Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/ carers is required.
- Setting mobile phones and devices must only be accessed or used by members of staff.
- Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in Appendix 1.
- Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.
- Setting mobile phones and devices will always be used in accordance with the ICT Security Acceptable Use policy and other relevant policies.

13. 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.
 - Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.

- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or a deputy DSL) will seek advice from the LA Education Safeguarding Service.
- Where there is suspicion that illegal activity has taken place, we will firstly contact the LA Education Safeguarding Service for advice, and then ~~or~~ Surrey 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 will speak with ~~Surrey Police or~~ the LA Education Safeguarding Service first to ensure that potential investigations are not compromised.

13.1 Concerns about Learners Welfare

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

13.2 Pupil Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

13.3 Staff Misuse

- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Disciplinary and Capability Policy and Procedures, and the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the Allegations of Abuse against Staff Policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the Children's Single Point of Access (C-SPA).

14. Procedures for Responding to Specific Online Incidents or Concerns

14.1 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'
- Nutfield Church (C of E) Primary School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos,

sexualised online bullying, online coercion and threats, 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 Safeguarding and Child Protection Policy and Anti-Bullying policy.
- Nutfield Church (C of E) Primary School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Nutfield Church (C of E) Primary School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Nutfield Church (C of E) Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our Wellbeing and Relationships and Sex Education (RSE) and Health Education 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 a deputy DSL) and act in accordance with our Safeguarding and Child Protection Policy and Anti-Bullying Policy.
 - If content is contained on learners' electronic devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.
 - Provide the necessary safeguards and support for all pupils involved, such as 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 Work Service 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 a deputy DSL) will discuss this with the LA Education Safeguarding Service first, and then Surrey Police 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.

14.2 Youth Produced Sexual Imagery ("Sexting")

- Nutfield Church (C of E) Primary School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or a deputy DSL).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: '[Sexting in schools and colleges: responding to incidents and safeguarding young people](#)'.

- Nutfield Church (C of E) Primary School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
 - Act in accordance with our Safeguarding and Child Protection Policy and the relevant Surrey Safeguarding Children’s Partnership procedures.
 - Ensure the DSL (or a deputy DSL) responds in line with the [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Store the device securely.
 - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.
 - Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
 - Inform parents and carers, if appropriate, about the incident and how it is being managed.
 - Make a referral to Children’s Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
 - Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
 - Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
 - Review the handling of any incidents to ensure that best practice was implemented; the senior leadership team will also review and update any management procedures, where necessary.

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

- Nutfield Church (C of E) Primary School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

- Nutfield Church (C of E) Primary School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or a deputy DSL).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
 - We will ensure that the ‘Click CEOP’ report button used to report online child sexual abuse is visible and available to pupils and other members of our community. This is available to access direct from the online safety page on the school website.
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
 - Act in accordance with our Safeguarding and Child Protection Policy and the relevant Surrey Safeguarding Children’s Partnership procedures.
 - If appropriate, store any devices involved securely.
 - Make a referral to Children’s Social Work Service (if required/appropriate) and immediately inform Surrey police via 101, or 999 if a child is at immediate risk.
 - Carry out a risk assessment which considers any vulnerabilities of learner 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 pupils, such as, offering counselling or pastoral support.
 - Review the handling of any incidents to ensure that best practice is implemented; the Senior Leadership Team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
 - Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Service and/or Surrey Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Child Sexual Exploitation Team (CSE) at Surrey Safeguarding Children’s Board by the DSL (or a deputy DSL).
- If learners at other setting are believed to have been targeted, the DSL (or a deputy DSL) will seek support from Surrey Police and/or the Education Safeguarding Service first to ensure that potential investigations are not compromised.

14.4 Indecent Images of Children (IIOC)

- Nutfield Church (C of E) Primary School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

- We seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation (IWF) 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 a deputy DSL) will obtain advice immediately through Surrey Police and/or the LA Education Safeguarding Service.
- If made aware of IIOC, we will:
 - Act in accordance with our Safeguarding and Child Protection Policy and the relevant Surrey Safeguarding Children’s Partnership procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), and Surrey police.
- If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:
 - Ensure that the DSL (or a 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 a 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 Work Service (as appropriate).
 - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
 - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
 - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
 - Inform the Children's Single Point of Access (C-SPA) and other relevant organisations in accordance with our managing allegations against staff policy.
 - Quarantine any devices until police advice has been sought.

14.5 Cyberbullying

● 14.5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

Cyberbullying, along with all other forms of bullying, will not be tolerated at Nutfield Church (C of E) Primary School.

- **14.5.2 Preventing and addressing cyber-bullying**

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their class and the issue will be addressed in collective worship.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying as part of the Wellbeing curriculum.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

Full details of how we will respond to cyberbullying are set out in our Anti-Bullying Policy and the Children's Anti-Bullying Policy. Copies are available on the school website, and a paper copy from the School Office.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

14.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Nutfield Church (C of E) Primary School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or a deputy DSL) will obtain advice through the LA Education Safeguarding Service and/or Surrey Police.

14.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. Nutfield Church Primary School's contract with JSPC includes Lightspeed Systems filtering included with the Broadband package providing fully compliant web filtering based on a comprehensive education-specific database. The Lightspeed Systems Web Filter gives real time visibility of all activity on our school's network, provides notifications alerting teachers to suspicious search queries and enables temporary block categories at user, IP, group or domain level and fixed and mobile devices. Its reporting function is compliant with the Prevent Duty to prevent people from being drawn into terrorism. If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or a deputy DSL) will be informed immediately, and action will be taken in line with our Safeguarding and 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 Safeguarding and Child Protection and allegations policies.

15. Acceptable use of the internet in school

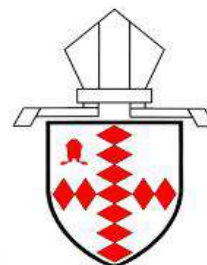
All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (Appendix 1). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.



NUTFIELD CHURCH (C OF E) PRIMARY SCHOOL



Nutfield Church (C of E) Primary School's Mission:

- We are a church school, which believes in the importance of **community**, where people from all races, religions and cultures act in **peace** together.
- Our pupils, staff and families work together as a team, with **wisdom** supporting each other through our learning. We have **hope** in our challenges and in our successes.
- We recognise the **dignity** and ultimate worth of each person created in the image of God, further shaped by the person, teaching and example of Jesus. We look to the future with **joy**.

ICT Security Acceptable Use – Staff, Governors and Volunteers

Nutfield Church Primary School will try to ensure that staff, governors and other volunteers have good access to digital technology to enhance their work, to enhance learning opportunities for pupils' learning and will expect staff, governors and other volunteers to agree to be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.

Nutfield Church Primary School aims to ensure that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk and that staff are protected from potential risk in their use of technology in their everyday work

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the system and other users. I recognise the value of the use of digital technology for enhanced learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will educate pupils in my care in the safe use of digital technology and embed online safety in my work with our children, staff, Governors and volunteers

- I understand that the school will monitor my use of the school digital technology and communications systems
- I will not disable or cause any damage to school equipment
- I will immediately report to the School Business Manager any damage or faults involving equipment or software, however this may have happened.
- I understand that the rules set out in the agreement also apply to use of these technologies out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use
- I will not disclose my user names or passwords to anyone else. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will not engage in any on-line activity that may compromise my professional responsibilities

- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted or I have any concerns about the validity of the email
- I will ensure that I will only use my school email address for all electronic communications with pupils, staff, parents, Governors or other volunteers and that all communications are compatible with my professional role
- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not give out my personal details such as mobile phone numbers and personal email address to pupils or parents
- I will only use the school's digital technology resources and systems for professional purposes.
- I will only use the approved, secure e-mail system for any school business.
- I will not browse, download or send materials that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate person.
- I will not allow unauthorised individuals to access email / internet / intranet / network of other school systems.
- I will not download any software or resources from the internet that can compromise the network, or are not adequately licensed.
- I understand that all internet usage can be logged.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, a laptop or other device to the network that does not have up-to-date anti-virus software.
- Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with the school's Online Safety and Acceptable Use Policy and Safeguarding Policy
- I will not use personal digital cameras or camera phones for transferring images of pupils or staff without permission.
- I will use the school website in accordance with school policy.
- I will ensure that any private social networking sites that I create or contribute to or belong to have appropriate levels of security and are not confused with my professional role.
- I will not conduct any communication with a current or ex-pupil via a social network site, such as Facebook, Twitter, Instagram, and Snapchat. Where an ex-pupil is a relative permission should be sought from the Headteacher.
- I agree and accept that any computer or laptop loaned to me by the school is provided solely to support my professional responsibilities.
- I understand that the school's Data Protection Policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system will be kept private and confidential.
- I will ensure that I am aware of digital safeguarding issues and will embed them within my classroom practice.
- I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I understand that failure to comply with the Acceptable Use Policy could lead to disciplinary action.

I agree to abide by the school's Online Safety and Acceptable Use Policy.

Signature

Date

Full Name

Job Title / Role.....

Nutfield Church (C of E) Primary School

Use of mobile phones in school

Staff should never contact children, young people or their families from their personal mobile phone, or give their mobile phone number to pupils. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.

Mobile phones will not be used during teaching periods in classroom environments or around the school where pupils may be working unless permission has been granted by a member of the senior leadership team in emergency circumstances.

Staff should only make use of mobile phones in designated areas. The designated area is the staff room or staff offices. If a private call needs to be made then a request for a room can be made to the Senior Leadership Team or the school office.

Staff should not use personal devices such as mobile phones or cameras at any time to take photos or videos of pupils.

Staff should not send and receive texts in lessons.

Staff will be issued with a school phone where contact with pupils, parents of carers is required, for example, a mobile on school trips or staff based landline in school offices. Where staff members are required to use a mobile phone for school duties, for instance in case of an emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone will be provided and used.

Staff should ensure that their phones and the school mobile are protected with PIN codes in case of loss or theft.

If a member of staff breaches the school policy then disciplinary action will be considered.

I agree to abide by the school's Policy on use of mobile phones in school.

Signature

Date

Full Name

Job Title.....

Nutfield Church (C of E) Primary School

Pupil Acceptable Use Agreement

- ✓ I will only use IT in school for school purposes.
- ✓ I will only use approved e-mail addresses for sending messages
- ✓ I will only open attachments from people I know, or who my teacher has approved.
- ✓ I will not tell other people my passwords.
- ✓ I will only open / delete my own files.
- ✓ I will make sure that all my contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless it is approved by an adult and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- ✓ I know that my use of IT can be checked and that my parent / carer contacted if a member of school staff is concerned about my online-safety.
- ✓ I will hand in any electronic devices I bring to school to the office e.g. iPad, mobile phone or Kindle.

I have read the acceptable use policy and agree to follow it.

Signed

Date

Name

Class

Nutfield Church (C of E) Primary School - Key Stage One Online Safety Charter.



Nutfield Church (C of E) Primary School – Key Stage 2 Charter – In Internet Awesome

https://storage.googleapis.com/gweb-interland.appspot.com/en-us/hub/pdfs/2021/BIA_Curriculum_June-2021_EN_PDF-Version.pdf



Be Internet Awesome.

Appendix 6

Nutfield Church Peace-Makers' Charter

We're a good school and so
no one should be bullied.

Treat others as you would like to be treated and try to show others the grace that
God shows to us.

All bullying will be noticed and
people will put a stop to it.

We do not think it is cool to be a bully.

At Nutfield Church we are all different
and we like it that way.

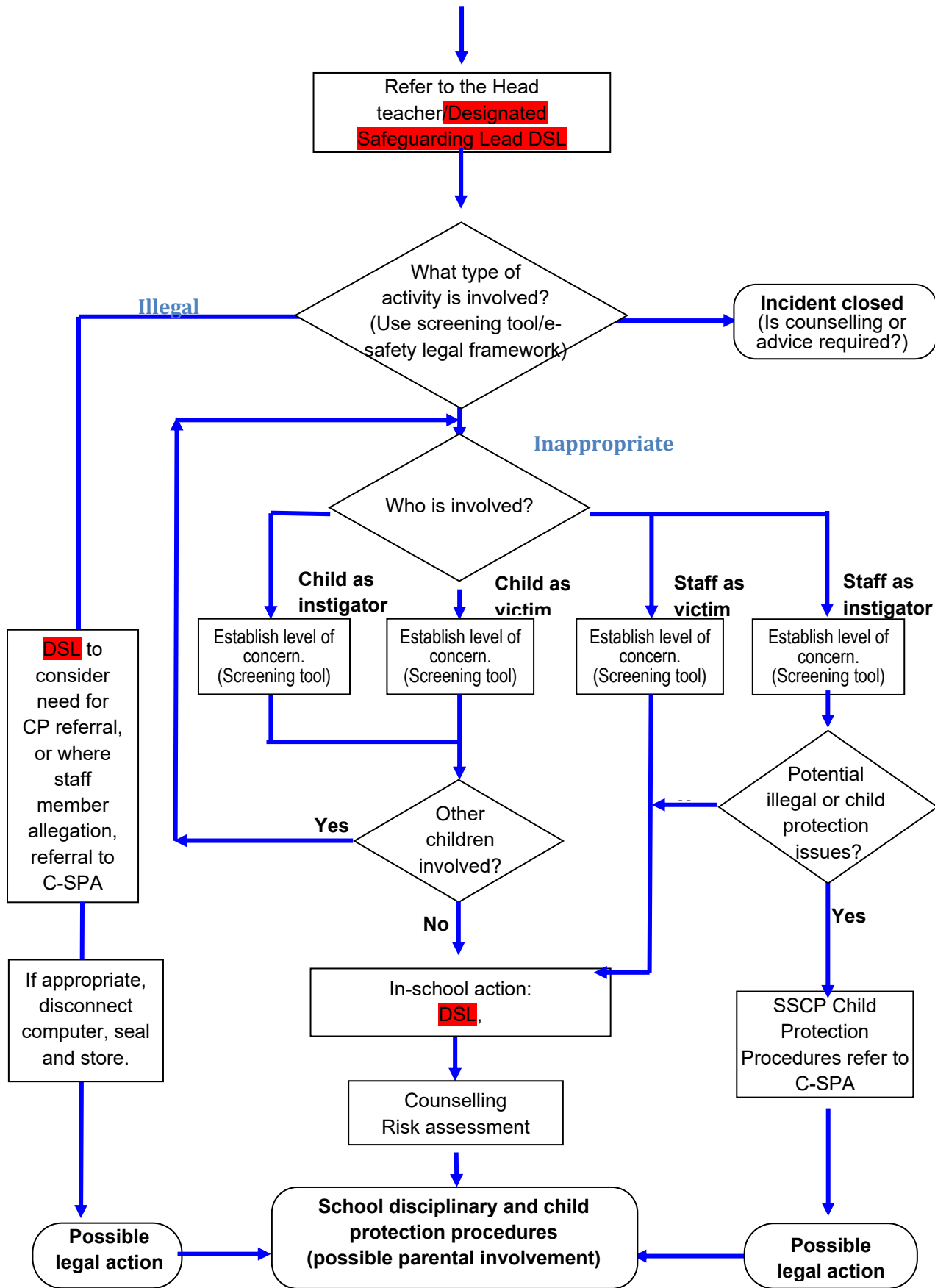
Choosing to be kind is helpful and necessary.

Appendix 7

What to do if you have an **online safety concern:**

A concern is raised

**Children's Single Point of Access
(C-SPA): 0300 470 9100**





Consent form for taking and using photos

Child's name:

Date:

Dear Parents/Carers

At Nutfield Church (C of E) Primary School, we take photographs and film pupils as part of our core activity of education. During your child's time at Nutfield Church (C of E) Primary School this occurs as part of normal teaching, learning, assessment and safeguarding procedures and as such we do not need your permission for these activities.

However, we do seek your permission to take photographs of your child and use them in the ways described below. Please consider carefully the ramification of not granting permission before you decide.

Why are we asking for your consent again?

You may be aware that new data protection rules came in from 25th May 2018 (GDPR). To ensure Nutfield Church (C of E) Primary School meets the new requirements, we need to obtain your consent under the new regulations to take and use photos of your child.

We really value using photos of your child to showcase what they do in school and demonstrate what school life is like to other stakeholders and the wider community, so we really appreciate you taking the time to give consent again.

Furthermore, it is hugely beneficial to be able to identify children with educational, dietary or medical needs to all staff, to safeguard and ensure their well-being.

Please tick all the relevant boxes, sign each item below and return this form to the school office.

I give consent for my child's photo to be stored in SIMS (School Information Management System) as part of their individual data file.

YES NO Signed.....

I give consent for my child's photograph to be taken by the school photographer, J P Photographic Limited for individual, group, class and whole school photographs.

YES NO Signed.....

I give my consent for photos and videos of my child to be used on the school website (name will be omitted).

YES NO Signed.....

I give my consent for photos of my child with their name to be used in classroom, corridor and entrance displays.

YES NO Signed.....

I give my consent for photos and the name of my child to appear in local newspapers and magazines. Please note that some newspapers may require the child's full name and may store photographs for online use.

YES NO

Signed.....

I give my consent for my child to be photographed and filmed by staff and fellow parents during school productions and events as long as it is made clear each time that these must only be used for personal viewing purposes and must not be published in any format including on-line.

YES NO Signed.....

I give my consent for my child's image to be used for identification purposes should they have a specific educational, dietary or medical need which needs to be communicated to all staff for safeguarding purposes. (These photographs will be displayed in the staff room and school kitchen only).

YES NO Signed.....

I give my consent for my child's named image to be taken by the adult in charge on school trips or visits

(The image would only be used in the event of an emergency and is shredded on return to school).

YES NO Signed.....

I give permission to participate in video conferencing. (Occasionally your child's class may talk to other children or an author for example, outside of the school under the supervision of their Class Teacher).

YES NO Signed.....

Please note: this form is valid for the period of time your child is on roll at Nutfield Church (C of E) Primary School. Where the consent is given for a specific reason e.g. a trip, medical condition etc. once this need ends the image will be destroyed by shredding.

If you wish to make any changes, please email the school office at info@nutfield.surrey.sch.uk or call the school on 01737 823239 and we will supply you with a new form. If you have any questions, please contact the school office.

Imogen Woods
Headteacher

Daniel Walker-Cheetham
Data Protection Officer

Parent or carer's signature: _____

Date: _____

Relationship to named child: _____