



Nether Kellet Primary School

Online Safety

This policy has been produced with reference to the DFE Online Safety advice and CEOP current advice and should be read in conjunction with the Computing and Anti-bullying policies.

Aims:

The Head and Governors of NKCPS recognise the importance of e-learning and the significant benefits presented to pupils, staff and parents by the emerging technologies used at home, at school and in the workplace. There are also significant risks inherent in the use of these technologies and this policy aims to minimise these risks by:

- ensuring that all with responsibilities in the area of online safety clearly understand their roles and duties
- explaining the school's approach to online safety
- providing a framework for the handling of online safety incidents

This policy should be read in conjunction with other school policies, particularly the Anti-Bullying Policy, Acceptable Use Policies, Behaviour Policy and Safeguarding Policy.

Communication:

Appropriate elements of the online safety policy will be shared with pupils.

The online safety policy will be available to parents on the school website.

Pupils and staff will be informed and regularly reminded that network and internet use will be monitored.

Opportunities to gain awareness of online safety issues and how best to deal with them will be provided for pupils. This should be addressed each year as pupils become more mature and the nature of newer risks can be identified.

This policy will be displayed on the safeguarding noticeboard and its importance explained to staff by the head teacher. All teaching and classroom support staff will sign to acknowledge that they have read and understood the online safety policy.

Responsibilities:

Governors

The Chair of Governors is responsible for appointing an online safety Governor, with lead responsibility for online safety, who will:

- review this policy at least annually and as necessary in response to any online safety incident to
- ensure that the policy is up to date and covers all aspects of technology use within the school.
- keep up to date with emerging risks and threats through technology-use and receive termly updates from the Head in regards to training, identified risks and any incidents
- keep the Chair of Governors and fellow Governors updated on online safety matters
- at governor meetings, monitor online safety through the head's reports which will detail whether online safety issues have occurred and, if so, how they have been dealt with to ensure the policy was effective and appropriately applied in managing those incidents.

Head

The head has overall responsibility for online safety within the school and will:

- keep up to date with emerging risks and threats through technology use;
- ensure they have had appropriate training and professional development in order to undertake the role;
- ensure that all online safety incidents are dealt with promptly and appropriately;
- allocate necessary resources to online safety on the advice of DFE guidelines, Lancashire LA guidelines and school's ICT support technicians;
- ensure online safety training throughout the school is planned and up to date and appropriate to the recipient: pupils, staff and governing body;
- keep up-to-date with the latest risks to children whilst using technology and with the latest research and available resources for school and home use;
- engage with parents and the school community on online safety matters at school and at home;
- liaise with Lancashire Safeguarding online safety team, IT technical support and other agencies as required;
- retain responsibility for the logging of any online safety incidents: where these are revealed through weekly filtering checks, they are logged on the filtering check form, where individual children are

involved and there are concerns around their use of ICT/safety, etc. issues are logged on CPOMs and reported to parents as appropriate;

- report to governors on online safety issues;
- review this policy regularly taking into account any issues or incidents.

The head is advised by an external team of IT consultants who, in collaboration with the head, ensure that:

- the IT technical infrastructure is secure;
- anti-virus is fit-for-purpose, up-to-date and applied to all capable devices;
- operating systems updates are regularly monitored and essential updates applied;
- online safety technical solutions such as Internet filtering or iPad central control systems are operating correctly and safely;
- filtering levels are applied appropriately and according to the age of the user and that categories of use are discussed and agreed with the online safety coordinator and Head;
- passwords are applied correctly to all users regardless of age;
- the Head is alerted as a matter of urgency to any vulnerability, security breach, attack or incident known to have caused or likely to have caused (including 'near misses') an online safety risk to pupils or staff (through checks made by the IT technician or by the head herself);
- advice on technical matters of online safety is provided to staff when required;
- IT System Administrator security is in place (to include the regular changing of administrator passwords);
- patterns of pupil and staff use of the network are regularly monitored;
- any issues related to data protection are referred to the head;
- the head and external IT technician review the filtering system on a weekly basis to ensure that the filters are working currently and, where necessary, the head investigates any apparently inappropriate searches that have been blocked by the filter.

All Staff

All teaching and classroom support staff are users of the network and have signed Acceptable Use policies which must be followed. They are also responsible for ensuring that:

- they understand all details within this policy. If anything is not understood it should be brought to the attention of the Head or online safety co-ordinator.
- they understand what cyber-bullying is and respond according to the Anti-Bullying Policy.
- any online safety incident is reported as quickly as possible to the DSLs. (The head is also lead DSL and online safety coordinator).

- they seek any support, training or advice they require in this rapidly changing area from the online safety co-ordinator
- they report any copyright or plagiarism issues to the Head

Staff are reminded that online safety incidents often involve safeguarding issues; school safeguarding procedures must be followed.

All Pupils

Pupils are responsible for their behaviour on the network and devices provided by the school just as they are in a classroom, the corridor, playground or other school grounds.

In order to use the network and devices provided by the school, pupils sign Acceptable Use policies and these must be followed. The boundaries of use of ICT equipment and services for pupils at NKCPs are given in the Student Acceptable Use Policy; breaking these rules or misusing ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

Cyber-bullying is when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else. (Childline 2013)

Pupils should:

- understand what cyber-bullying is
- understand that the school will not tolerate cyber-bullying and that pupils who cyber-bully, particularly when this is repeated or aggressive in nature, can expect to be punished by school.
- understand that being a 'bystander' or passing on images or messages created by cyber-bullies could itself be defined as cyber-bullying.
- be aware that if investigation of an online safety incident suggests that a pupil's misbehaviour may be criminal or pose a serious threat to a member of the public, the Head will contact the Police.

When pupils have a concern or a questions about:

- how others are treating them.
- how a friend or another pupil is being treated.
- their own behaviour

they are expected to bring this promptly to the attention of a teacher or parent so that help, support and advice can be provided. They are reminded of the need to do this within all internet safety teaching sessions, assemblies and Kidsafe sessions as well as incidentally on frequent occasions when using ICT.

Parents and Carers

The school recognises that emerging technologies present significant challenges to parents who often have questions or concerns about online safety and the school will aim through website updates, PING messages,

leaflets and newsletters to keep parents up to date with new and emerging online safety risks, and involve parents in strategies to ensure that pupils are empowered.

NKCPS strongly recommends that parents follow the advice provided by CEOP (Child Exploitation Online Protection) via the website www.thinkuknow.co.uk as this provides regularly updated information for parents of children of all ages and useful age-appropriate material to look at together with your children. School also recommends that parents install parental controls on all devices accessible to their children and monitor what is being accessed online and, where this is taking place, communications between their child and others online.

Through assemblies, computing lessons, cross-curricular lessons and the PSHE programme, online safety is taught both discretely and embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff and made aware of how they can report areas of concern whilst at school or outside of school. Parents should be aware that evidence of cyber-bullying taking place outside of school may result in school sanctions.

NKCPS takes a proactive approach to online safety. Parents should note however that many areas including:

- the number of hours children spend on the internet or using mobile devices at home;
- the hours during which children are permitted access to the internet or mobile devices at home;
- the types of interaction on the internet permitted (e.g. unregulated contact with peers, contact with strangers) at home;
- the security settings and permissions on home equipment and devices
- adherence to gaming/video/social networking age guidelines, regulations and laws;
- permission to join social networking sites or online gaming or chat;

are parenting decisions around which the school can provide advice but over which the school ultimately has no control. It is absolutely essential, therefore, that parents exercise vigilance and take responsibility for these vital aspects of modern family life.

Parents are responsible for:

- bringing swiftly to the attention of the head any online safety concerns including concerns over cyber-bullying or inappropriate uses of digital technology.
- counter-signing the Student Acceptable Use Policy before their child accesses school ICT equipment or services

Parents are reminded that, as in all parenting matters, values and practices vary significantly from family to family. When their children visit friends' homes, parents are advised to discuss in advance with the friends' parents

their expectations for access to and use of technology (e.g. mobile phone access, gaming, internet use, DVD age ratings).

Where minor difficulties arise between children of families known to each other in the offline world, parents can often deal with these by sensitive contact with the parents of the child concerned. It will be helpful to keep the school informed of any relevant information. In the event that this approach is not possible or desirable, parents can seek advice from the head. In a serious case which might involve criminal offence or risk to an individual, parents or the school may need to contact agencies such as CEOP (via their website) or the Police; when a child is in immediate danger, 999 should be called.

Parents with concerns, questions or suggestions regarding online safety are encouraged to contact the head who will be happy to discuss these and to provide advice. **Parents and staff are advised that they must not forward to the school digital material (e.g. an offensive image sent to their child) which they believe to be offensive or criminal in nature as this action may in itself constitute a criminal offence.**

AI

As AI becomes more widespread, more used and more sophisticated, school is aware of some of the risks that this may pose. Vigilance is exercised in terms of the children's use of the internet and they are taught to be sceptical of what they see and read as part of online safety education. Our safeguarding policy specifically refers to detailed protocols around AI use and for the pupils a key element of this can be the deepfake aspect, both in terms of what they encounter and also potentially in terms of creating such media themselves. Pupils are taught throughout school to report to adult anything they believe to be false and potentially harmful to themselves and others. They are also taught to be very selective about what they put on line and obtain permissions first. Staff exercise caution about their use of AI including ensuring that no personal data or work belonging to a child is copied into an AI app and no information is shared on AI that is personal to children, staff, school or any individuals associated with school. Where children's images are posted on our website and subsequently on social media, staff are vigilant in ensuring that no names accompany pictures, similarly, when names are mentioned, no pictures accompany them.

Prevent Duty for Schools

For access to all online content, the school is protected by a secure filtering system. In addition to this, staff closely monitor any content that children access and children are educated on an ongoing basis (with focused lessons each term and specific focus during Internet Safety Week) how to use the internet safely and what to do in the event that they encounter something they are uncomfortable with. This includes content designed to influence

behaviours and attitudes such as radicalisation materials. Children are taught in an age-appropriate way about types of internet content that isn't appropriate. In addition to this, through Philosophy 4 Children, PSHE and Global Learning, children are taught to approach all ideas and information with a critical approach. In Kidsafe training, children are taught how to be safe online and how to deal with issues that may arise. Where internet content is encountered that is relevant to the Prevent agenda this will be reported to the head as DSL.

Mobile Devices

Children are not permitted to use their own mobile devices in school and are discouraged from bringing them to school. On the odd occasion that a child needs to bring a mobile phone to school for a specific reason, this is looked after by office staff and returned to the child at the end of the school day. Staff are permitted to use mobile phones in school only as per the staff Code of Conduct.