Online-Safety Policy

This policy applies to all members of Northcott School who have access to and are users of schools ICT systems.

Policy Introduction

Northcott's online-safety policy has been written to ensure online safety measures are in place to protect both pupils and staff working with ICT equipment and related technologies. The policy is to assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own and pupils' standards and practice. Our responsibility is to set high expectations of our pupils using communication technologies and to maintain a consistent approach to online safety by knowing the content of the policy and the procedures adopted and developed by the school.

Scope of Policy

- This policy applies to the whole school community including Northcott's Senior Leadership Team, school governors, all staff employed directly or indirectly by the school and all pupils.
- Northcott's senior leadership team and school governors will ensure that any relevant or new legislation that may impact upon the provision for eSafeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are away from the school site. This is pertinent to incidents of cyberbullying, or other eSafeguarding related incidents covered by this policy, which may take place out of school, but which are linked to membership of the school.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate eSafeguarding behaviour that take place out of school.

Review and Ownership

- Northcott's eSafeguarding policy has been written by the school eSafeguarding Coordinator together with the Child Protection Coordinator, and is current and appropriate for its intended audience and purpose.
- Northcott's eSafeguarding policy has been agreed by the senior leadership team and approved by governors.
- Northcott's eSafeguarding policy will be reviewed annually or when any significant changes occur with regards to the technologies in use within the school.
- The School has appointed a member of the governing body to take lead responsibility for eSafeguarding.

- Amendments to the school eSafeguarding policy will be discussed in detail with all members of teaching staff.

The Responsibility of the Senior Leadership Team

We believe that eSafeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

- The head teacher is ultimately responsible for safeguarding provision (including eSafeguarding) for all members of the school community, though the day-to-day responsibility for eSafeguarding will be delegated to the eSafeguarding coordinator.
- The head teacher and senior leadership team are responsible for ensuring that the eSafeguarding Coordinator and other relevant staff receive suitable training to enable them to carry out their eSafeguarding roles and to train other colleagues when necessary.
- The senior leadership team will receive updates from the eSafeguarding Coordinator when appropriate.
- The head teacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident.
- The head teacher and senior leadership team should receive update reports from the incident manager.

The Responsibility of the ESafeguarding Co-ordinator

- To be the designated Senior Information Risk Officer (SIRO) for the school.
- To promote an awareness and commitment to eSafeguarding throughout the school.
- To be the first point of contact in school on all eSafeguarding matters.
- To take day-to-day responsibility for eSafeguarding within school and to have a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- To have regular contact with other eSafeguarding committees, e.g. the local authority, Local Safeguarding Children Board (along with the Child Protection Coordinator).
- To communicate regularly with the school ICT technical support.
- To communicate regularly with the designated eSafeguarding governor.
- To communicate regularly with the senior leadership team
- To create and maintain eSafeguarding policies and procedures.
- To develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in eSafeguarding issues.
- To report annually to governors about eSafeguarding
- To ensure that eSafeguarding education is embedded across the curriculum.
- To ensure that eSafeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.

- To monitor and report on eSafeguarding issues to the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- To understand the issues surrounding the sharing of personal or sensitive information.

Responsibility of Teachers and Support Staff

- To read, understand and help promote the school's eSafeguarding policies and guidance and sign to confirm they have read them.
- To read, understand and adhere to the school staff Acceptable Use Policy
- To ensure that any eSafeguarding incidents are reported in accordance with the school Behaviour Policy and that the eSafeguarding Coordinator is copied into the slips.
- To develop and maintain an awareness of current eSafeguarding issues and guidance.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. email, text, mobile phones, social networking etc. Please see Social Networking Guidance.
- To embed eSafeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide pupils carefully when engaged in learning activities involving technology.
- To ensure that pupils are fully aware of research skills and methods.
- To be aware of eSafeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms that exist within the school.
- To maintain a professional level of conduct in personal use of technology at all times.

Responsibility of Technical Staff: RM

- To be aware of the school's eSafeguarding policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- To develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.

- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Responsibility of Pupils

- Certain categories of pupils within school will understand and adhere to the school pupil Acceptable Use Policy. The Provision and Primary pupils will have one format , KS3 pupils will have a more advanced format and KS4 will have a higher level format
- Pupils who are unable to understand the AUP may require a parent/ guardian to sign on their behalf.
- To help and support the school in the creation of eSafeguarding policies and practices and to adhere to any policies and practices the school creates.
- Where appropriate pupils will be expected to understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school rules relating to bullying and cyberbullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to understand the incident-reporting mechanisms that exists within school.
- To discuss eSafeguarding issues with family and friends in an open and honest way.
- Elected class representatives will attend termly meetings of the eSafeguarding committee.

Responsibility of Parents and Carers

- To help and support the school in promoting eSafeguarding.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.

- To discuss eSafeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology.
- To consult with the school if they have any concerns about their children's use of technology.
- To sign the home-school agreement upon admission.
- To sign the photography permission form stating where photographs are to be published upon admission.

Responsibility of Governors

- To read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
- One governor will have responsibility for eSafeguarding.
- To develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- To develop an overview of how the school ICT infrastructure provides safe access to the internet.
- To develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- To support the work of the eSafeguarding committee in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
- To ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.
- To develop an overview and understanding as the body corporate in relation to their responsibilities regarding the schools Data Protection commitments.

Responsibility of Child Protection Officer

- To understand the dangers regarding access to inappropriate online contact with adults and strangers.
- To liaise regularly with the eSafeguarding Coordinator.
- To be aware of potential or actual incidents involving grooming of young children.
- To be aware of and understand cyberbullying and the use of social media for this purpose.

Responsibilities of other External Groups

- The school will liaise with local organisations to establish a common approach to eSafeguarding and the safe use of technologies.
- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate.
- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds. (parent helpers, trainee teachers, work experience pupils).

Managing Digital Content

- Before photographs of pupils can be published, permission must be granted formally via the photography permission form, which has to be signed by parents upon induction. All staff are aware of the process involved with publishing images over different mechanisms.
- Parents and carers may withdraw permission, in writing, at any time. A procedure exists for permission to be removed retrospectively.
- We will remind pupils of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Pupils and staff will only use school equipment to create digital images, video and sound. In exceptional circumstances, personal equipment may be used with permission from the head teacher provided that any media is transferred solely to a school device and deleted from any personal devices. In particular, digital images, video and sound will not be taken without the permission of the person with parental responsibility; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online other than on the school website in accordance with the photography permission form.
- Parents may take photographs at school events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites (optional - unless appropriate security settings are enabled and set to maximum). This is in accordance with the parental agreement letter signed upon admission.
- When searching for images, video or sound clips, staff will be taught about copyright and acknowledging ownership.
- When searching for images, video or sound clips staff will ensure that pupils' usage is monitored for copyright purposes.

Storage of Images

- Any images, videos or sound clips of pupils must be stored on the school network / storage devices and never transferred to personally-owned equipment. These should be stored in areas which pupils are not able to access. If pupils need access to these for specific learning activities, they can be given this but they must be deleted after use. The school will store images of pupils that have left the school for a number of years following their departure for use in school activities and promotional resources.
- Individual staff members have the responsibility of deleting the images when they are no longer required, or when a pupil has left the school. This instruction will come from a member of the Senior Leadership Team once a procedure and agreement has been decided.

Online sexual harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded or humiliated and/or create a hostile, offensive or sexualised environment. Online sexual harassment, which might include: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as

'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats.

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our school follows and adheres to the national guidance - UKCCIS: Sexting in schools and colleges: Responding to incidents and safeguarding young people, 2016.

Teaching and Learning

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.
- Pupils will be taught about the impact of bullying and cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

Staff Training

- Our staff receive regular information and training on eSafeguarding issues in the form of annual updates and when appropriate.
- As part of the induction process all new staff receive information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate eSafeguarding activities and awareness within their curriculum areas.

Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.

- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- Members of staff will access the network using an individual username and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the network through their username and password. They will abide by the school A.U.P. at all times.
- All pupils, when appropriate, will have a unique username and password for access to ICT systems.

Passwords

- A secure and robust username and password convention exists for all system access. (email, network access, school management information system).
- All information systems require staff to change their password at first log on. Where appropriate pupils will be assisted by members of staff in this particular task.
- Staff should change their passwords whenever there is any indication of possible system or password compromise.
- Pupils' passwords will be managed by the appropriate member of support / teaching staff and changed when is deemed appropriate.
- All staff have a responsibility for the security of their username and password. Staff must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Staff are expected to comply with the following password rules:

1. Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
2. Always use your own personal passwords to access computer based services, never share these with other users.
3. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures).
4. Never save system-based usernames and passwords within an internet browser.

New Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view. We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafeguarding risk.

- The school will audit ICT equipment usage to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- Methods to identify, assess and minimise risks will be reviewed regularly.

Mobile Phones

- Any pupil who brings his or her mobile phone or personally-owned device into school should switch it off and hand it into staff until the end of the day.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised to contact the school reception if the need arises.

Staff Use of Mobile Devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will use a school phone to contact parents or carers.
- Mobile Phones and personally-owned devices will be stored securely with personal belongings.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Filtering Internet Access

The school filters its internet provision. The filtering system is provided by **eSafe Forensic Monitoring.**

- The school's internet provision will include filtering appropriate to the age and maturity of pupils. The ICT Coordinator is able to contribute to filtering by reporting inappropriate content to 'smoothwall' via the RM reporting system.
- The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.
- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding Coordinator. The school will report such incidents to appropriate agencies including the filtering provider, the local authority or CEOP.
- The school will regularly review the filtering product for its effectiveness.
- Any amendments to the school filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Pupils will be taught to assess content as their internet usage skills develop.
- Pupils will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Internet Access Authorisations

- All parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- Parents will be asked to read the school Acceptable Use Policy for pupil access and discuss it with their children, when and where it is deemed appropriate.
- All pupils will have the appropriate awareness training through eSafeguarding lessons and, where possible, sign the pupil Acceptable Use Policy prior to being granted internet access within school.
- All staff will be offered eSafeguarding training, which will be updated annually, and sign the staff Acceptable Use Policy prior to being granted internet access within school.
- Parents will be informed that pupils will be provided with supervised internet access appropriate to their age and ability.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- Any visitor who requires internet access will be asked to read and sign the Acceptable Use Policy which is in the induction pack.
- When considering internet access for vulnerable members of the school community (looked after children) the school will make decisions based on local knowledge.
- All pupils will be closely supervised and monitored during their use of the internet. Pupils will be frequently reminded of internet safety issues and safe usage.

Email

- Staff should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Staff should not use personal email accounts during school hours or for professional purposes, especially to exchange any school-related information or documents.
- Access, in school, to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and productivity and will be restricted in line with the school eSafeguarding and Acceptable Use Policies.
- The school gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the online safety and security of users and recipients, all mail is filtered and logged. A full audit trail can be made available should this become necessary.
- School email accounts should be the only account that is used for school-related business.
- Staff will only use official school-provided email accounts to communicate with pupils and parents and carers, as approved by the senior leadership team and the SIRO.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Irrespective of how staff access their school email (from home or within school), school policies still apply.

- Emails sent to external organisations should be written carefully and professionally to protect the member of staff sending the email.
- Chain messages will not be permitted or forwarded on to other school-owned email addresses.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Staff who send emails to external organisations, parents or pupils, are advised to carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- All emails that are no longer required or of any value should be deleted.
- Staff should check email accounts regularly for new correspondence.
- Emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies needs to be controlled and never communicated through the use of a personal account.
- Staff will be made aware of the dangers of opening email from an unknown sender or source or viewing and opening attachments.
- All email and email attachments will be scanned for malicious content.
- Staff should never open attachments from an untrusted source.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of staff immediately.
- All email users within school should report any inappropriate or offensive emails through the Local Authority incident-reporting system.
- Pupils must immediately tell a teacher or trusted adult if they receive any inappropriate or offensive email.
- KS4 pupils will be allocated an individual email account for their own use in school or class.
- Pupils may only use school-provided email accounts for school purposes.
- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages.
- Pupils and staff will be reminded about the dangers of revealing personal information within email conversations.
- Pupils must not reveal personal details of themselves or others in email communications. Pupils should get prior permission from an adult if they arrange to meet with anyone through an email conversation.

Using Blogs, Wikis, Podcasts and Other Mechanisms to Publish Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website/ blog and postings should be approved by the head teacher before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.

- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside school.

Use of Social Media

- Staff must not talk about their professional role in any capacity when using personal social media such as Facebook and YouTube or any other online publishing websites.
- Staff and pupils are asked to report any incidents of cyberbullying to the school.
- Staff will raise any concerns about pupil use of social media sites with parents/carers this includes the use of any sites that are not age appropriate.
- All staff will receive training on the risks associated with the use of social media either through staff meetings or via the induction process for new starters. Safe and professional behaviour is outlined in the Acceptable Use Policy.
- Staff must not use social media tools to communicate with current or former pupils.
- Staff will not use any social media tools to communicate with parents.
- Procedures for dealing with cyberbullying incidents of staff or pupils involving social media are outlined in the school Anti-Bullying policy.
- Staff are advised to set and maintain profiles on such sites to maximum privacy and to give access to known friends only.

Data Protection and Information Security
Please refer to the school Data Protection Policy

Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT items are disposed of by authorised companies who will supply a written guarantee that any content is removed.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007.

Special Requirements
We will seek to ensure that all users have access to ICT through the use of a range of specially adapted hardware.

Reviewed: December 2018

Approved by Governors:

Next Review: December 2019