CANTRELL PRIMARY
AND
NURSERY SCHOOL

Online Safety Policy
Including Filtering & Monitoring
2023/24

Next review date: Autumn 2024

Online Safety Policy

Here at Cantrell Primary and Nursery School we want to provide a safe caring environment for our children, where they feel safe, nurtured and happy.

In order to achieve this, we have in place a group of policies that complement each other to safeguard, protect and promote the welfare of our children.

These policies are:

Computing Policy

Behaviour Policy

SEND Policy

Safeguarding Policy

Confidential Reporting Code (Whistle Blowing Procedure)

GDPR Acceptable Use Policy

PSHE Policy

Anti-Bullying Policy

Social Media/Networking Policy

Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Cantrell Primary and Nursery School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.

The main areas of risk for our school community can be summarised as follows:

- Exposure to inappropriate content.
- Lifestyle websites promoting harmful behaviours.
- Hate content.
- Content validation: how to check authenticity and accuracy of online content.
- Online bullying in all forms
- Social or commercial identity theft, including passwords.
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information.
- Digital footprint and online reputation.
- Health and well-being (amount of time spent on-line, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership).

Scope

This policy applies to all members of Cantrell Primary and Nursery School (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Cantrell Primary School IT systems both in and out of school.

It reflects the latest guidance in Keeping Children Safe in Education 2023 and Meeting the Digital standards in School and Colleges 2023.

Roles and Responsibilities Headteacher

- Must be adequately trained in off-line and online safeguarding, in line with statutory guidance.
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.
- To take overall responsibility for online safety provision.
- To take overall responsibility for data management and information security, ensuring school's provision follows best practice in information handling.

- To ensure the school uses appropriate IT systems and services including, filtering and monitoring.
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.
- To be aware of procedures to be followed in the event of a serious online safety incident.
- Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including the risk of children being radicalised.
- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures, e.g. Schools IT.
- To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangement for online safety.
- To ensure the school website includes the relevant information.

Computing Lead

- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy.
- Promote an awareness and commitment to online safety policy/documents.
- Promote an awareness and commitment to online safety throughout the school community.
- Ensure that online safety is embedded within the curriculum.
- Liaise with Schools IT.

DSLs

- Take day to day responsibility for online safety issues
- Take lead responsibility for overseeing filtering and monitoring reports
- Check filtering and monitoring reports and share updates with governors
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident.
- To ensure that online safety incidents are logged as a safeguarding concern.
- Facilitate training and advice for all staff.
- Liaise with the Local Authority and relevant agencies.
- Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles.

Governors

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve the Online Safety Policy and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in online safety activities

Schools IT

- To report online safety related issues that come to their attention, to the Head teacher.
- To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date)

- access controls/encryption exist to protect personal and sensitive information held on school-owned devices - the school's policy on web filtering is applied and updated on a regular basis

- That they keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Head teacher
- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the school's online security and technical procedures
- Maintain the schools filtering and monitoring system- Smoothwall
- Provide reports on filtering and monitoring
- Complete actions following concerns or checks to the system

Teachers

- To embed online safety in the curriculum
- To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities when relevant)
- Report concerns via My Concern where they see or suspect unacceptable content has been accessed
- To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
- Report to lead DSL if they perceive that there are any unreasonable restrictions which inhibits their ability to teach a broad and balanced curriculum
- Liaise with DSL if they are teaching content which may result in a spike in filtering and monitoring logs
- Report any abbreviations or misspellings which allow access to inappropriate content.
- Ensure that there is a log of which devices children have used during each lesson

All staff, volunteers and contractors

- To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually.
- To report any suspected misuse or problem as a safeguarding issue
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology

Exit strategy

- At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils

- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- To contribute to any 'pupil voice' / surveys that gathers information of their online experiences

Parents/carers

- to consult with the school if they have any concerns about their children's use of technology
- to support the school in promoting online safety.

Handling Incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- A DSL acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to a DSL (and if relevant Schools IT) that day
- Any concern about staff misuse is always referred directly to the Head teacher, unless the concern is about the Head teacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude selfie incident:

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people. When assessing the risks the following should be considered:
- Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
- Who has shared the imagery?
- Where has the imagery been shared?
- Was it shared and received with the knowledge of the pupil in the imagery?
- Are there any adults involved in the sharing of imagery?
- What is the impact on the pupils involved?
- Do the pupils involved have additional vulnerabilities? Does the young person understand consent?
- Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming. If none of the above apply, then school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light). The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is

confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support.

Reviewing and Monitoring Online Safety

The online safety policy is supported within other school policies (including the Safeguarding and Child Protection policy, Anti-Bullying policy, PSHE policy, ICT policy).

- The online safety policy will be reviewed bi-annually or when any significant changes occur with regard to the technologies in use within the school
- There is widespread ownership of the policy and it has been agreed by the SLT.

All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of the Computing curriculum and PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- makes regular training available to staff on online safety issues.
- provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the school's Acceptable Use Policy

Parent awareness and training

This school:

- runs workshops on online safety advice, guidance and training for parents.
- Provide information through newsletters, website and curriculum activities.

Expected conduct:

In this school, all Staff and Children:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- Staff, volunteers and contractors know and understand school policies on the use of mobile and hand held devices including cameras;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;
- Are aware that the above-expected conduct relates to use of technology at home, particularly when using email, blogs, Purple Mash and TEAMS.

Parents/Carers:

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online safety acceptable use agreement form; (appendix A)
- have signed the pupil acceptable use policy.

Incident Management In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (i.e. the local authority, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Internet access, security (virus protection) and filtering This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through Schools IT;
- uses Smoothwall which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status. Smoothwall is also used to monitor internet usage
- ensures network health through the use of anti-virus software (from Schools IT);
- Uses DfE, LA approved systems to send secure file/email data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with Schools IT to ensure any concerns about the system are communicated so that systems remain robust and protect students.

To ensure the network is used safely, this school:

- Ensures staff read the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network;
- Ensures that a log is kept detailing who has used each computer
- All year groups have their own unique username and password which gives them access to the Internet and other services;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;

- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any laptop or i-pad loaned to them by the school, is used primarily to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted
- IT and communications systems have all been installed professionally and are regularly reviewed to ensure they meet health and safety standards;

Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to use STRONG passwords.
- We require staff to change their passwords every 90 days

E-mail

This school:

- Provides staff with an email account for their professional use, this is through Schools IT using a Nottingham City Staff email and makes clear personal email should be through a separate account;
- Will contact Schools IT, and if applicable, the Police, if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LA or Schools IT e mail systems on the school system
- Staff will use Schools IT e-mail systems for professional purposes only

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

School Shared Drive

- Uploading of information on the schools' learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community;

Social networking Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- the use of any school approved social networking will adhere to school's social media and networking policy.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Head teacher.
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils

Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:

- Parents are reminded about social networking risks and protocols when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school. (See mobile phone policy)
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.
- Any device brought into school by a pupil must be handed in to their teacher and collected at the end of the school day.
- Staff members may use their phones during school break times in the staff room.
- If a staff member is expecting a personal call they may seek specific permissions to use their phone at other than their break times.
- All visitors are requested to keep their phones on silent.

- The recording, taking and sharing of images, video and audio on any personal mobile device is not prohibited.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families within or outside of the setting except for during off-site activities where contact with a parent or carer may be required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Head teacher and/or DSL.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff read the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- The school blocks/filter access to social networking sites;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.