Creswell C of E
Infant and Nursery School

Online Safety Policy

Creswell C of E Infant & Nursery School

Review every 2 years by IT/Full Governors

Date of review	Comments	Signed by Chair of Governors	Date
June 2017	Rejected July 2017		
March 2018	Rejected 15/03/18		
May 2018	Approved July 2018		
November 2020	Approved November 2020		
May 2022	Approved May 2022		
June 2024	Approved 20th June 2024		

Creswell C of E Infant and Nursery School

Online Safety Policy

Introduction

These guidelines have been drawn up to ensure that all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead. We are in the process of establishing good protocol by using the 360 degree Safe self-evaluation tool. (https://360safe.org.uk/Accreditation)

This policy is to also ensure we safeguard pupils within all aspects of the ever-changing online world.

At Creswell C of E Infant and Nursery School we ensure that Online is given a high profile in the following ways:

- Online is taught throughout the pupil's Computing and PSHE sessions as necessary.
- We provide KS1 pupils with assemblies each half term, to teach about Online. These are reviewed regularly to ensure that they are up-to-date, child friendly and reflect current needs.
- Pupils are taught how to act online and how to minimise the risk when working on the internet and different forms of technology.
- Pupils are taught about managing individual passwords, respecting copyright and other elements of this policy that are relevant to them.
- Parents are provided with resources to support Online at home and are encouraged to take responsibility for their online presence, respecting the opinions and privacy of others and modelling good behaviour to children.
- Training is provided for staff and governors on a regular basis to ensure that they conduct themselves in the appropriate manner when working and communicating online.
- If there is a website available to pupils that staff deem inappropriate they should report it to the Computing Coordinator and the Head Teacher and record it in the Computing Incident Log Book.
- If pupils need to talk to someone about an experience online that worries them, they should talk to the Computing Coordinator, a member of the safeguarding team or other appropriate adult.
- Cyber-bullying issues are followed up thoroughly and in accordance with the anti-bullying policy

- To report a worry or concern about a child's safety online, parents can access the CEOP button on the creswell-inf.derbyshire.sch.uk website, which will link to: https://www.ceop.police.uk/safety-centre/

Aims/Rationale

Computing encompasses every part of modern life and it is important that our pupils are taught how to use these tools and more importantly, how to use them safely. We believe that it is important for pupils, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent independent users and learners of Computing we aim to:

- Use Computing where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
- Use Computing to help improve standards in all subjects across the curriculum
- Develop the Computing competence and skills of pupils through Computing lessons and provide them with the chance to consolidate these in a cross-curricular context
- Ensure pupils are challenged in their use of Computing and are provided with exciting, creative ways in which to share their learning
- Use tools available to ensure pupils have the ability to work independently and collaboratively to suit the needs of the situation
- Provide all staff with the training and support to ensure that they can, and have the confidence to, use Computing to its full potential in all aspects of school life
- Use Computing as a form of communication with parents, pupils and the wider community
- Ensure online safety has a high priority in school
- Ensure pupils have the appropriate life skills with technology and online safety

Roles and Responsibilities

Governors: Governors are responsible for the approval of the Online Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governing Body receiving regular information about online incidents and monitoring reports.

School: As a school, we endeavour to ensure that parents and pupils are aware of ways in which the internet and Computing can be used productively and safely. We ensure that we provide pupils with the opportunities to excel and achieve when using Computing and that our curriculum is challenging and relevant. Before launching any system or

initiative, we make sure that the pupil's safety is at the forefront of our thoughts and we keep parents informed as necessary through newsletters and parent events. A range of online safety websites and sources of support are made available via links on the school website. We will conduct an annual survey of parents and pupils to ascertain internet use at home.

Head Teacher / Designated Safeguarding Lead:

- As Designated Safeguarding Lead, is responsible for ensuring the safety (including online) of all members of the school community.
- Is responsible for ensuring staff receive suitable training to enable them to carry out their Online roles and to train other colleagues, as relevant.
- Will ensure that there is a system in place to allow for the monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Will receive regular monitoring reports Computing Lead (Deputy Head Teacher).

Computing Lead / Deputy Head Teacher

- Takes day to day responsibility for Online issues and has a leading role in establishing and reviewing the school's online safety policy
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff
- Liaises with the Local Authority
- Liaises with school Computing technician
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Reports regularly to the Head Teacher

Computing Technician is responsible for ensuring that:

- The school's Computing infrastructure is secure and is not open to misuse or malicious attack
- Users may only access the school's networks through a properly enforced password protection policy
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- The use of the network/Virtual Learning Environment (VLE)/ remote access/ email is regularly monitored in order that any misuse/ attempted misuse is

reported to the Computing Lead (Deputy Head Teacher) and Designated Safeguarding Lead (Head Teacher).
- Monitoring software/ systems are implemented and updated

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Computing Lead (Deputy Head Teacher) and Designated Safeguarding Lead (Head Teacher) for investigation/ action/ sanction. Reports for pupil's should be logged on CPOMs. Reports for staff should be sent via encrypted email.
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Pupils understand and follow the school online safety and acceptable use policies
- They monitor Computing activity in lessons, extra-curricular and extended school activities and report where appropriate
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Students / visitors: if either a visitor or student wishes to have an account to logon to the school network, they should speak to a member of the Senior Leadership Team / Computing Lead. Staff are aware of the safeguarding duties outlined in the Safeguarding Policy.

Pupils: Pupils should read or have read to them, understand and sign the school pupil Acceptable Use Policy (AUP) which should then be displayed in each classroom. They should follow the guidelines laid out in the AUP. They should ensure that they use the computers and equipment appropriately at all times. It is expected that pupils will follow the school's behaviour policy when working online. They are also expected to adhere to the school's Anti-bullying policy. If the pupils fail to do so, then the procedures outlined in these policies will come into force.

Parents: Parents should stay vigilant to the websites and content that their pupils are accessing. They should also try to talk to their child about online safety and the use of the internet. Parents are encouraged to take responsibility for their online presence, respecting the opinions and privacy of others and modelling good behaviour to children. If they have any questions or concerns then they should speak to their child's teacher,

the Computing Lead (Deputy Head Teacher) or the Head Teacher. Parents should report all concerns via a concerns form or via our email address.

School Website and Blogs (Linked to 360Safe Public Facing and Professional Standards Guidelines)

The school website is overseen by the Head Teacher. Class pages and any subject specific pages will be updated by the class teacher and / or the subject leader. The current website is hosted by eSchools.

Internet and Email

The internet may be accessed by staff and by pupils at any time. Staff are always vigilant as to the sites pupils are accessing and pupils should not be using the internet unattended. Pupils are not allowed to have personal mobile phones or other similar devices in school.

The teaching of email and internet use will be covered within the Computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of teaching staff and certain members of the support staff are issued with a school email address which is the email address they should use for all professional communication. ClassDojo is the primary tool for day to day communication with parents. Staff should take extra care to ensure that all communication with pupils and/or parents remains professional. Social media should never be used for professional communication except for the school's Facebook page and Twitter account. Users are responsible for all messages that are sent and due regard should be paid to the content of emails and messages to ensure it is not misconstrued.

All web activity should be logged off appropriately after use.

The use of the internet to access inappropriate materials such as auction sites, pornography, racist or other material is prohibited on school equipment or on personal devices using the school WiFi. If users, especially pupils, do see an inappropriate website or image, they should close this immediately and report the site to their class teacher and/or the Computing Lead.

The internet and filtering is provided by RM using Netsweeper and inappropriate websites are filtered out. Additional sites can be enabled by the Computing technician and a record will also be kept of the sites enabled by school. Any websites utilised to support learning, that require any personal information or passwords setting up for staff or pupils, will be assessed by the Data Protection Officer (School Business Manager) by completing a Data Protection Impact Assessment (DPIA) with Derbyshire County Council before use of the website. This is in line with the Data Protection Policy 2018.

Digital and Video Images (Linked to 360Safe Digital and Video Guidelines)

We will ensure that if we publish any photographs or videos of pupils online, we:

- Will try to ensure that their parents or guardians have given us written permission
- Will ensure if we do not have permission to use the image of a particular child, we will make them unrecognisable to ensure that they are not left out of situations unnecessarily
- Will not include a child's image and their name together
- Will ensure that pupils are in appropriate dress
- If a parent, guardian or child wishes, they can request that a photograph is removed. This request can be made verbally or in writing to the child's teacher or to the Computing Lead. We will endeavour to remove the photograph as soon as possible
- Will provide new parents with a photo permission letter upon their arrival into school
- Will ask parents or guardians that are recording video or taking digital images at public events e.g. school play or sports day, that they do not publish these online
- Staff are allowed to take digital/ video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.

Passwords (linked to 360Safe Password Guidelines)

Staff should ensure that any passwords they use are strong and contain a mixture of some of the following; upper and lower-case letters, numbers and special characters. These should be changed regularly, especially if the user suspects others may know the password.

Curriculum

Online Safety is a focus in all areas of the curriculum and staff will reinforce online safety messages in the use of Computing across the curriculum in the following ways:

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the pupils visit.

- Pupils are taught in all lessons to be critically aware of the materials/ content they access online
- Pupils will understand that Online is an important part of the world we live in. Being 'e-safe' is something we have to think about and be aware of, every time we use a piece of technology
- Teachers will follow online safety curriculum

Remote Learning

When there is a need to access the curriculum remotely, such as Covid-19 self isolation or school shutdowns, staff, pupils and parents will be guided to the Remote Learning policy which incorporates online safety.

Sustainability and Environmental Impact

- To ensure that the level of computing across the school is sustainable the Computing Lead is responsible for the upkeep of the Electronic Computing Handbook which will contain usernames, passwords and guides to online tools and software as well as details of licenses and a complete ICT inventory.
- Hardware is disposed of safely and securely through an approved company

Complaints

Incidents regarding the misuse of the Internet by pupils will be logged on CPOMs and alerted to the Designated Safeguarding Lead (Head Teacher) who will decide which additional evidence should be gathered or recorded. A partnership approach with parents will be encouraged. Complaints of cyber-bullying are dealt with in accordance with our anti-bullying policy. Any complaint about staff misuse will be referred to the Head Teacher. Complaints of a child protection nature must be dealt with in accordance with child protection procedures.

Copyright and Intellectual Property Right (IPR)

Copyright of materials should be respected. This includes when downloading material and/or copying from printed materials. Staff should not remove logos or trademarks unless the terms of the website allow it.

Staff should check permission rights before using materials, particularly images, from the internet. Pupils are taught to begin to consider the use of images from the internet.

All materials created by staff whilst in employment of the school belong to the school and should not be used for financial gain. This in accordance with Local Authority guidelines. We will continue to update staff, pupils and parents of any updates.

Responding to unacceptable use by staff

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly the law.

Responding to unacceptable use by pupils

Pupils should be aware that all Online issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and, if necessary, the anti-bullying policy. Pupils may have restrictions placed on their access to equipment for a short time.

Review Date: 26th November 2025