eSafety Policy

Review date: 31st of March 2020

Next review date: 30th of March 2021

Contents

This is a trust-wide policy and all schools in Cirrus Primary Academy Trust must follow this policy. The terms school and academy are used in this document to mean the educational establishment in the Trust.

1. Introduction

This policy is part of the school's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's safeguarding and child protection processes.

2. Aims

At Cirrus Academy Trust, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the school communities in its safe and responsible use of technology
- Establish clear mechanisms to identify and deal with incidents

3. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, *Keeping Children Safe in Education*, and its advice for schools on preventing and tackling bullying and guidance on protecting children from outside influences such as radicalisation serious violent crime. The policy takes into account the Teaching Online Safety in School (DfE June 2019), National Curriculum Computing programmes of study and PSHE recommendations. It also reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate content on pupils' electronic devices, in line with the DfE's advice for schools on searching, screening and confiscation.

4. Roles and Responsibilities

4.1 All governors will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the Internet

The Head teacher is responsible for ensuring staff understand this policy and that it is being implemented consistently throughout the school.

4.2 The Designated Safeguarding Lead (DSL) will:

- Have overarching responsibility for E-Safety
- Work with the other staff (Head teacher and E-Safety/Computing Lead), as necessary, to address any online safety issues or incidents that have a child protection concern
- Liaise with other agencies and/or external services if necessary
- Report on online safety in school to the Head teacher and/or governing board
- Identify particular incidents related to E-Safety for staff training purposes and this will contribute to developments in policy and practice in online safety within the school

4.3 The DSL/E-Safety/Computing Lead will:

- Update and deliver staff training on online safety and ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Ensure that online safety education is embedded within the curriculum
- Ensure that online safety incidents are logged by the Designated Safeguarding Lead (DSL) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying and peer on peer abuse are logged and dealt with appropriately in line with the school Behaviour Policy
- Communicate regularly with the Senior Leadership Team (SLT) to discuss current issues and review incident logs

4.4 Teachers will:

- Teach and embed the E-Safety curriculum as set out in the Computing and PSHE overviews
- Supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant).

4.5 All staff and volunteers will:

- Read, ensure they understand, sign and adhere to the school Staff Acceptable Use Agreement (AUP)
- Ensure that online safety incidents are dealt with and logged appropriately by the Designated Safeguarding Lead (DSL) or nominated member of staff from the Safeguarding Team, in line with this policy and that they are reported, where necessary, to the E-Safety/Computing Lead
- Model safe, responsible and professional behaviours in their own use of technology

4.6 The ICT Service Manager will:

- Put in place appropriate filtering, blocking and monitoring systems, which keep pupils safe from potentially harmful and inappropriate content and contact online whilst at school, including terrorist and extremist material
- Ensure that the school's ICT systems are secure and protected against viruses and malware

4.7 Parents/Carers are expected to:

- Ensure their child has read, understood and is adhering to the Pupil Acceptable Use Agreement
- Ensure they have read, understood and is adhering to the Parent/Carers Acceptable Use Agreement
- Support the school should an issue arise

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

UK Safer Internet Centre: www.saferinternet.org.uk
Childnet International: www.childnet.com
NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
Net Aware: https://www.net-aware.org.uk
Think U Know: www.thinkuknow.co.uk
Digizen: www.digizen.org

5. Educating Pupils about Online Safety (Linked to Relationships Education Scheme of Work)

Pupils are specifically taught about safe use of the internet. Our policy is only to allow access to certain sites however, it is impossible to block everything – we teach pupils what is acceptable and what is unacceptable, and what to do when they feel 'uncomfortable'.

Assemblies and guest speakers may also be used to educate pupils about the risks that can be encountered online. Pupils are taught about safeguarding issues, including how technology can provide a platform for issues such as Child Sexual Exploitation, radicalisation and sexual predation. Pupils are taught about the safe use of social media and, using age-appropriate resources, are taught how to stay safe from radicalisation, Child Sexual Exploitation, FGM, grooming and peer-on-peer abuse. We use the curriculum to ensure that children and young people understand how people with extreme views share these with others, especially using the internet. Pupils are equipped with the skills needed to feel safe and adopt safe online practices to help them recognise online risks and stay safe from abuse.

Pupils in EYFS and Key Stage 1 are taught:

- To use technology safely and respectfully, keeping personal information private
- To identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 are taught:

- To use technology safely, respectfully and responsibly
- To recognise acceptable and unacceptable behaviour
- To identify a range of ways to report concerns about content and contact

The breadth of issues classified with online safety can be categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views
- **Contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults and
- **Conduct:** personal online behaviour that increases the likelihood of, or causes harm; for example making, sending and receiving explicit images, or online bullying

6. Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. See also the school Behaviour Policy.
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to themselves or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than a victim.

Emotional abuse may involve serious bullying (including cyberbullying), causing children frequently to feel frightened or in danger, or the exploitation or corruption of children.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. The DSL and E-Safety Lead will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

7. Safeguarding

The first indication of concern about a pupil's welfare is not necessarily the presence of an injury. Signs that could be an indication of abuse may include:

- Misuse of information technology (e.g. Youth Produced Sexual Imagery, inappropriate comments on Social Media, texting, cyberbullying and online grooming)

8. Monitoring and Filtering

When pupils use the school's network to access the internet, they are protected from inappropriate content by our filtering and monitoring systems. However, some pupils are able to access the internet using their own data plan (e.g. if a child in Year 5/6 brings in their mobile phone – see below about mobile phones). To minimise inappropriate use, pupils are supervised and guided carefully when engaged in learning activities involving online technology. Online safety education is embedded within the curriculum and pupils are taught how to use online technology safely and responsibly. The school will ensure that the use of filtering and monitoring systems does not cause 'over blocking' which may lead to unreasonable restrictions as to what pupils can be taught regarding online teaching.

9. Email

All staff use the Trust's Office 365 for email, and all KS2 pupils use LGfL's Londonmail for email (EYFS and KS1 if applicable). Both systems have virus and malware scanning on every email, as well as 'rude word' checking, etc. Any emails found to exceed the threshold (set at '3') are flagged up and reported to the authorised users. Authorised users have the ability to look at any emails within both systems. Other webmail systems are blocked.

10. Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 and the Education Act 2011 to search for, and if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with a member of the Senior Leadership Team to decide whether they should:

- Delete the material
- Retain it as evidence (of a criminal offence or a breach of the school rules)
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's guidance on screening, searching and confiscation.

11. Mobile phones and Smart Watches

Only children in Year 5 and 6 are able to have a mobile phone in school. Children are not allowed to wear Smart Watches to school. If they choose to bring a mobile phone into school it must be left with the class teacher/school office for the duration of the school day. If the phone is used inappropriately the child will not be able to bring the device into school again, as signed for in the Acceptable Use Agreement. It is the child's responsibility to hand their phone in to their class teacher/office. The school takes no responsibility for loss or theft. Mobile phones will be kept securely and returned before the end of the day.

12. Acceptable Use of the Internet

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (see appendices). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. More information is set out in the acceptable use agreements in the appendices.

13. Responding to Issues of Misuse

Clear processes are in place to identify and deal with incidents effectively. All pupils, parents and staff sign an Acceptable Use Agreement. Where a pupil misuses the school's ICT systems or the internet, the action taken will depend on the individual circumstances, nature and seriousness of the specific incident. Each school will follow the procedures set out in their Behaviour Policy and/or the following:

- Incidents will be reported to the E-Safety Lead/DSL
- Where pupils have breached the Acceptable Use Agreement, this will be managed within the behaviour policy and procedures for each individual School
- Parents/Carers will be informed of online safety incidents involving children for whom they are responsible
- The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the appropriate authorities – police, Internet Watch Foundation, CEOP
- Incidents are monitored by the E-Safety Lead/DSL and any learning points are used to develop staff training, pupil education or parent awareness e.g. specific lessons are taught relating to the breach; external speakers are invited in to speak about specific topics; additional parent workshops are held for a particular year group etc.

14. Training

All staff members will receive training, including refresher training, at least once every academic year, on safe internet use and online safeguarding issues including cyber-bullying and risks of online radicalisation. They will receive relevant updates as required, e.g. through emails and staff meetings. All staff members will be made aware of the following:

- Pupil attitudes and behaviours which may indicate that they are at risk of potential harm online.

- The procedure to follow when they have a concern regarding a pupil's online activity.

15. Staff use of mobile phones and cameras

- Trust staff and members of the Senior Leadership Team may have mobile phones on them at all times.
- Other staff members will not use personal mobile phones or cameras when pupils are present.
- Staff may use mobile phones on school premises outside of working hours when no pupils are present (unless in emergency cases where this has been discussed and agreed by a member of the Senior Leadership Team).
- Staff may use mobile phones during breaks and non-contact time as long as no children are present (unless in emergency cases where this has been discussed and agreed by a member of the Senior Leadership Team).
- Staff will use their professional judgement in emergency situations.
- Staff may take mobile phones on trips which should only be used in emergencies. Staff may be able to use their mobile phones on trips at the discretion of the Senior Leadership Team.
- Personal mobile devices will not be used to take images or videos of pupils or staff in any circumstances unless agreed with the Senior Leadership Team.
- Staff will adhere to the E-Safety Policy at all times.
- Photographs and videos of pupils will be carefully planned before any activity with particular regard to consent and adhering to the school's Data Protection Policy.
- Where photographs and videos involve CLA (Child Looked After) pupils, adopted pupils or pupils for whom there are security concerns, a member of the Senior Leadership Team will liaise with the Designated Safeguarding Lead to determine the steps involved. The DSL will, in known cases of a pupil who is a LAC or who has been adopted, liaise with the pupil's social worker, carers or adoptive parents to assess the needs and risks associated with a pupil.
- Staff will report any concerns about another staff member's use of mobile phones to the Designated Safeguarding Lead.

16. Related Policies

- Trust Safeguarding & Child Protection Policy
- Annex to Safeguarding and Child Protection Policy
- Anti Bullying
- Behaviour
- Keeping Children Safe in Education (Part 1 and Annex A)
- Safe Working Practise Agreement

Appendix 1: Acceptable Use Agreement (Parents/Carers)

At Name School, we ensure that all pupils have good access to digital technologies to support their teaching and learning and we expect all our pupils to agree to be responsible users in order to keep everyone safe.

At school your child will be asked to read (or will have read to them) and sign an Acceptable Use Agreement tailored to his/her age. Please read this carefully – it is attached in Appendix 2 or 3.

Agreement

I understand that my child has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

As the parent/carer of the pupil below, I understand that my son/daughter will have access to the internet and to ICT systems at school and is expected to follow the Acceptable Use Agreement.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that children will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that the school takes inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. I understand that my child's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I understand that only children in Year 5/6 are able to have a mobile phone in school. If I choose for my child to bring a mobile phone into school it must be left with the class teacher for the duration of the school day. I understand that it is my child's responsibility to hand their phone in to their class teacher and that the school takes no responsibility for loss or theft. I understand that if the phone is used inappropriately, my child will not be able to bring the device into school again.

I will support the school by promoting safe and responsible use of the internet, online services and digital technology at home and will inform the school if I have concerns.
I understand that if I take photographs or videos at school events that have other children or staff in them, I will not share these online without their permission.

Name(s) of pupil(s): _____ Child's Class(s): _____

Parent/Carer Name: _____

Parent /Carer Signature: _____

Date: _____

Appendix 2: Pupil Acceptable Use Agreement EYFS and Key Stage 1

This agreement will help keep me safe and help me to treat others respectfully.

This is how I will keep safe online:

Name of Pupil:	Date:
Class:	

This is how I **keep safe** online:

- ✓ I will only use the devices and websites my teacher says I'm allowed to use.
- ✓ I will check before I use new sites, games or apps.
- ✓ I will remember that people online aren't always who they say they are and will not arrange to meet them.
- ✓ I won't change clothes in front of a camera or send photos of myself or others.
- ✓ I won't share my personal information (including my name, address, telephone number, usernames, passwords, religion, ethnicity or health information).
- ✓ I will be kind and polite to people online and will not join in with bullying.
- ✓ I will tell a trusted adult if I am worried, scared or just not sure.

My Trusted Adults are:

At School_____

_____

At Home _____

_____

Appendix 3: Pupil Acceptable Use Agreement Key Stage 2

This agreement will help keep me safe and help me to treat others respectfully.

This is how I will keep safe online:

Name of Pupil:	Date:
Class:	

This is how I **keep safe** online:

- ✓ I use the school's internet and devices for schoolwork and other activities to **learn** and have fun.
- ✓ I will not use the school systems or devices without a trusted adult giving me **permission** and being present
- ✓ I only **use** sites, games and apps that my trusted adults say I can
- ✓ I won't **share** anything that I know another person wouldn't want shared, or which might upset them
- ✓ I **keep** my passwords to myself and ask for them to be reset if anyone finds them out
- ✓ I think before I **click** on links
- ✓ I **understand** that some people might not be who they say they are
- ✓ I do not share **private** information
- ✓ I keep my **body** to myself online
- ✓ I don't **send** any photos without checking with a trusted adult
- ✓ I ask to **talk** to a trusted adult if I am upset, worried scared or unsure
- ✓ I know that some apps, games, websites and social networks have age **restrictions** and **rules** on how to behave and I respect this
- ✓ I am **considerate**, **respectful** and **kind** online
- ✓ I keep **others safe** by talking to a trusted adult if I am worried about something I see or hear
- ✓ I will **not meet** with anyone I speak to online that I do not know in real life
- ✓ I can say **no** online if I need to and do not have to do something just because a 'friend' asks me to.

My Trusted Adults are:

At School_____

_____

At Home _____

_____

I understand that if I breach the rules, I may not be allowed to use the internet for a period of time as determined by my teacher. I will also take part in an E-Safety reflection session where I will discuss appropriate use of the internet, watch videos or take part in additional learning activities based on the breach I took part in. My teacher will help me fill in a reflection sheet during the activity saying what I have learned about how to behave online in future. I have read and understood this agreement.

Appendix 4: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

When using the school's ICT systems and accessing the internet in school, or outside school on a work device:

- I understand that it is a criminal offence to use a school computing system or service for a purpose not authorised by its owner and this shall be for business and professional use only
- I appreciate that ICT encompasses but is not limited to computing equipment, mobile telephones, personal organisers, digital cameras, printers, fax machines, the Internet, email, social networking and that it may also include personal ICT devices when used for school business
- I understand that school information systems must not be used for private purposes without specific permission from the Head Teacher and that use for personal financial gain, gambling, political purposes, personal interests or advertising is forbidden
- I understand that my use of school information systems, Internet and email are monitored and recorded to ensure policy compliance
- I will respect system security and will not disclose or cause to be disclosed any password or security information to anyone other than an authorised system manager
- I will not use, install or alter any software or hardware without permission, including the use of personal memory sticks or other portable media
- I will ensure that personal data is stored securely and used appropriately, whether in school, off the school premises or accessed remotely
- I will ensure that no personal data is taken off site or transmitted externally without first encrypting the information to the AES 256 standard or higher and will NOT use a personal USB stick in school
- I will respect copyright and intellectual property rights
- I will ensure that business and personal electronic communications including email, instant messaging and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted
- I will not "friend" a pupil on my personal social networking web site, blog or other service
- I will promote online safety with pupils in my care and will help them to develop a responsible attitude to ICT and Internet use, communications and publishing
- I will ensure that my personal mobile phone or other electronic devices are switched off or locked away during all times that I have contact with children during the school day. Personal mobile phones should only be used in the staff room, outside the premises or other designated area agreed with SLT
- I will not use a personal mobile phone device to contact pupils or parents and I will not disclose my personal telephone number or contact details to pupils or parents
- I will not engage, at any time, in exchanges with pupils on social networking sites or internet chatrooms. This may lead to disciplinary proceedings
- I will not, at any time, post photographs that include other members of staff anywhere on the internet without their written permission. This may lead to disciplinary proceedings.
- I will not use any personal electronic device to take photographs or videos of pupils, unless authorised to do so by the Head teacher

- I will not, at any time, post photographs or videos that include pupils anywhere on the internet, unless authorised to do so by the Head teacher. This may lead to disciplinary proceedings
- I will report any incidents of concern regarding pupil's safety or information security to the Online Safety Coordinator, Designated Child Protection Coordinator or Head Teacher. The school may exercise its right to monitor the use of the information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system is being used for criminal purposes or storage of inappropriate or unlawful text, imagery or sound. I have read, understood and accept the Staff ICT Acceptable Use Agreement

Name: _____

Signed: _____

Date: _____

Appendix 5: Online Communication (including Social Media) Code of Conduct for Staff Working with Children

This code of conduct is designed to protect all staff who use such sites in their private lives. As adults who work with children we have a duty to demonstrate the highest standards of conduct or integrity. We need to ensure that our actions in our private lives do not put us into situations where our conduct or integrity might be called into question or potentially bring our employer into disrepute. This could result in disciplinary action by your employer or even criminal prosecution. This code of conduct sets out expectations around your online behaviour that could affect professional standing, integrity and dignity.

Problematic usage of social networking could be:

- Staff referring to parents or children and young people by name
- Staff referring to forthcoming trips/visits
- Staff using derogatory or offensive language about parents, colleagues, managers, or the organisation for which they work
- Staff posting images of themselves in inappropriate dress or situations
- Staff posting images of pupils on the internet
- Staff participating in illegal activities such as the sharing of indecent images of children
- Partners or friends posting inappropriate comments concerning staff
- Partners and friends posting images that show staff members in situations which may not be in keeping with their professional status

What are we protecting?

- Ourselves as members of staff: our privacy, reputation and safety
- The children we work with: their privacy, reputation and safety
- The reputation of our employer

Code of conduct

- Staff should not enter into online contact with children (regardless of age) they work with, parents or their families. Friend requests from parents or children and young people under the age of 18 (past or present) in this context should be politely declined by explaining that it is against school policy, which is designed to protect staff from abuse and misunderstandings
- Staff should not create web pages, groups or contact lists concerning professional activities carried out on behalf of the school unless they have express written permission from a senior manager
- Staff should only make contact with children for professional reasons and in accordance with any organisational policy
- There must be absolutely no private online contact between staff and any children and young people with whom they have a work-related relationship.
- Staff should not store images or videos of any children or young people, with whom they have a work-related relationship, on their private machines
- Staff should not post images or videos of pupils, with whom they have a work-related relationship, on any social networking site/the internet
- Online contact made as part of professional duties should always be carried out using technologies provided by the school or local authority. These technologies should have the capability of logging and storing records securely. These emails should only be sent using Cirrus Trust email addresses and not other systems which aren't provided by the local authority for example Hotmail, Googlemail, MSN

- Staff are strongly advised to be careful about what they say online in contact with other young people such as relatives or family friends. This applies to any media, for example: images, audio or video material
- Any contact with children and young persons after they have left the organisation (e.g. moved to a secondary school) should be sanctioned by a senior manager within the organisation and the parent and not occur through social networking sites or other online communication technologies
- Staff should not give personal contact details to children and young people including their mobile telephone number and details of any blogs or personal websites
- Staff should not use internet or web-based communication channels to send personal messages to a child
- Ensure that if staff use a social networking site, details are not shared with children and young people and privacy settings are set at maximum

This code does not cover:

- Social contact between adult colleagues. However, staff need to be mindful of what they are posting and who can see it. This is important in respect of confidentiality, workplace relationships. Online contacts may not appreciate the difference between private and professional comments
- Membership of professional networks or forums: these are usually covered by a professional body's own code of conduct
- Membership of forums, although in extreme cases legal restrictions may apply. Staff should however remember that what they say may reflect upon their professional lives and moderate their comments accordingly
- Staff are strongly recommended to check that their online privacy settings only allow "friends" to see their profiles
- Staff are advised not to accept friend requests from people who are not personally known to them
- Staff should ask colleagues before photographs are posted which may cause them embarrassment. Staff posting their own images should bear in mind the fact that any image can easily be downloaded and manipulated and they should choose which images they share accordingly.
- It is recommended that staff do not post images that could be used to identify their homes or families
- All staff are advised to make themselves familiar with the parent/carer pages on the CEOP "Think U Know" site at www.thinkuknow.co.uk and keep themselves up to date with the risks of emerging technologies

Name: _____

Signed: _____

Date: _____