Acceptable Use of Technologies (Including Mobile Phones)

Introduction

New technologies have become integral to the lives of children and staff in today's society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.
In an ever-changing world, ensuring pupils' safety online has never been more important. It's an all-encompassing duty and something every teacher must be vigilant of.

Online Safety

We work hard to ensure that children are safeguarded from potentially harmful and inappropriate online material. We understand that an effective whole school approach to online safety empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

'Online safety refers to the act of staying safe online. It is also commonly known as internet safety, e-safety and cyber safety. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets. Being safe online means individuals are protecting themselves and others from online harms and risks which may jeopardise their personal information, lead to unsafe communications or even effect their mental health and wellbeing.'

(National Online Safety)

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

(KCSIE 2024)

We believe online safety:

- is an integral part of safeguarding and requires a whole school, cross-curricular approach
- must follow the school's safeguarding and child protection procedures
- will educate pupils about the benefits and risks of using technology
- will provide safeguards and awareness to enable pupils to control their online experience

At Cedars Primary and Nursery, we understand the responsibility to educate our pupils on online safety issues in accordance with the relationships education, relationships and sex education (RSE) and health education. Pupils are taught the principles of positive relationships online. Teachers address online safety and appropriate behaviours. Pupils are taught about how information and data is shared for example: sharing pictures, understanding that many websites are businesses and how sites may use information provided by users in ways they might not expect.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them. Staff receive regular training on compliance of GDPR matters.

Roles and Responsibilities

As online safety is an important aspect of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The designated safeguarding lead is the online safety co-ordinator who is supported by the IT technician. Together they are responsible for the filtering and monitoring systems within the school and regularly reviewing their effectiveness. All members of the school community have been made aware of who holds this post.

The senior leadership team and governors are updated by the Headteacher and governors so they understand the issues and strategies Cedars Primary and Nursery has in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Safeguarding: Child Protection, Health and Safety, Attitudes and Behaviour (including the anti-bullying) and Relationships, Sex and Health Education (RSHE).

Online Safety in the Curriculum

IT and online resources are used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded across the school and the principles of online safety are taught within computing and PSHE lessons as well as incorporated in the wider curriculum.

In accordance with the relationships education, relationships and sex education (RSE) and health education, pupils are taught:

- that people sometimes behave differently online, including by pretending to be someone they are not
- that the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- the rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- how to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- how information and data is shared and used online

Furthermore, our pupils are taught about elements of online activity that can adversely affect their wellbeing. They will identify and explore how to find a positive balance between time spent online and offline and recognise when activities stop being fun.

Pupils are taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are aware of where to seek advice or help if they experience problems when using the internet and related technologies: parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.

Educating pupils about the dangers of "sexting" (the making and distribution of self-taken images featuring nudity or explicit content) is part of the online safety curriculum (this is addressed with age-appropriate content).

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children.

E-Mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private.

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, 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 safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses. Staff must tell parents that all electronic communications should be via the office.
- E-mails created or received as part of staff roles will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage e-mail accounts as follows:
- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent housekeeping on all folders and archives

- The forwarding of chain letters is not permitted in school.
- All e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication or arrange to meet anyone without specific permission. Attachments should be checked for viruses. Emails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, emails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.
- Staff must inform the IT Technician and the Headteacher if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.
- However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending E-Mails

Staff must:

- Use their own school e-mail account so that they are clearly identified as the originator of a message
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate
- Not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments
- Not use the school e-mail for personal advertising

Receiving E-Mails

Staff must:

- Check their e-mail regularly
- Activate an 'out-of-office' notification when they are away for extended periods
- Never open attachments from an untrusted source; consult the IT Technician if there are any doubts
- Not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder
- Not automatically forward and delete e-mails

Online Safety Support for Staff

- Staff receive regular and appropriate information and training on online safety and how they can promote the 'Stay Safe' online messages. This is usually through a scheduled programme of staff meetings.
- New staff, students and volunteers (depending on their role) receive information on the school's staff code of conduct, online safety and acceptable use of technologies (including mobile phones) policies as part of their induction. Staff are asked to read this document each year.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.

The Internet

The internet is an open worldwide communication medium, available to everyone, at any time. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Cedars Primary School and Nursery follows the Department for Education's filtering and monitoring standards and the guidance in KCSIE 2024. The school has filtering and monitoring systems in place for all school devices and school networks and these are regularly reviewed. All use of the internet is logged and whenever any inappropriate use is detected it will be followed up.

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must always observe software copyright. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Online gambling or gaming is not allowed.
- All staff, volunteers and governors must comply with the social media guidelines the school has regarding the posting of any information or images relating to the school.
- School internet access is controlled through the E2BN's Protex Web filtering service. The service blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- Cedars Primary School and Nursery is aware of its responsibility when monitoring staff communication under current legislation (a record of all blocked sites, the date, who the user was and what action was taken by the online safety coordinator and/or IT technician is kept and reviewed regularly with the Headteacher).
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring computers and iPads.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the teacher and online safety coordinator or IT technician as appropriate.
- It is the responsibility of the school, to ensure that anti-virus protection is installed and kept up to date on all school machines.
- Pupils and staff are not permitted to download programs, files or apps on school-based technologies without seeking prior permission from the IT technician.
- If there are any issues related to viruses or anti-virus software, the IT technician should be informed.
- The school does not allow any access to social networking sites.

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school and to be aware of their responsibilities. We raise raise parents/carers' awareness of internet safety in newsletters, Parent Mail items (weekly 'Wake Up Wednesday' information from National Online Safety), our website and practical training sessions e.g. (Safer Internet Day, NSPCC).

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

- Staff and visitors are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Appropriate images can be taken using school iPods or iPads; these should be transferred as soon as possible to the school's network and deleted from the individual device.
- Pupils are not permitted to use personal digital equipment to record images of pupils, staff and others without advance permission from the Headteacher.
- Staff must have permission from the Headteacher before any image can be uploaded for publication.
- Permission to use images of all staff who work at the school is sought on induction and a copy can be found in their personnel file.
- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school web site.
- On the Learning Journeys – used by the Early Years Team.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- Recorded/ transmitted on a video or webcam.
- In display material that may be used in the school's communal areas.
- In display material that may be used in external areas, i.e. exhibition promoting the school.
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue e.g. divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting a child's work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Management of Applications (apps) used to Record Children's Progress (where used)

The school uses Target Tracker to track pupils progress and shares appropriate information with parents and carers.

The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking system is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation.

To safeguard pupils' data:

- Only school issued devices will be used for apps that record and store children's personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store children's personal details, attainment or images.
- School devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

Storage of Images

- Images/ films of children are stored on the school's network.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks).
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

Mobile Phones

The school allows staff to bring in personal mobile phones and devices for their own use. During the school day school staff are restricted to using their mobile phones to break times and lunchtimes with their mobile phones being switched off during lesson/work times. It is the responsibility of all school staff to keep their mobile phones securely stored.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on it.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- Staff are allowed only to use their mobile phones throughout the school day in the case of a personal emergency (this should be discussed with the Headteacher).
- Texts messaged should not be sent or received in lessons.
- Camera phones should not be used at any time to photograph a pupil.
- Content on the device.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- Mobile phones should not be used to send or receive inappropriate texts or images.
- Staff will not give email address to pupils or parents/carers.
- Staff are not to give out their mobile telephone number to parents or pupils.
- Staff will tell parents that all electronic communications should be via the office.
- Staff must use the school telephone to contact a parent and not use their mobile phone.
- Staff must not store parents or pupils telephone numbers on their mobile phones.
- Staff should not use personal mobile devices to contact a pupil or parent/carer unless in exceptional circumstances and with the prior approval of the Headteacher.
- Staff are not to be photographed by a parent or a pupil on a mobile phone.
- Staff will be issued with a school mobile phone when attending an off-site residential educational visit (this mobile phone is not for private use).
- Family members should be informed that in the case of an emergency that staff can be contacted through the school day via the school office.

Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to inform the school if they consent to images of their child being taken and used in the public domain (e.g., on school website).
- The school disseminates information to parents relating to online safety where appropriate in the form of newsletters, Parent Mail items, our website and practical training sessions.

Security

The school gives relevant staff access to its Management Information System, with a unique username and password.

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and this policy.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff should avoid leaving any portable or mobile IT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.
- Staff should always carry portable and mobile IT equipment or removable media as hand luggage and always keep it under their control.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents copied, scanned or printed.
- It is imperative that staff save data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is necessary to do so, the local drive must be encrypted.
- Privately owned IT equipment should not be used on a school network unless in exceptional circumstances and with the prior approval of the Headteacher. In these cases, devices should be connected to the "guest" Wi-Fi network only – this has limited accessibility.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles. When a device is left unattended, the screen should be locked to prevent unauthorised access.
- All IT equipment is security marked as soon as possible after it is received. The School Business Manager maintains a register of all IT equipment and other portable assets.
- IT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.
- On termination of employment, resignation or transfer, staff must return all IT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.
- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- The installation of any applications or software packages must be authorised by the IT technician.
- As a user of the school IT equipment, all staff are responsible for their activity.

Server Security

- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.
- Existing servers should have security software installed appropriate to the machine's specification and the school uses a remote back up service and data is backed up daily.

Using Removable Media

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by our IT technician.

Monitoring

- This policy (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).
- Internet activity is logged by the school's internet provider and in addition the school's technician regularly monitors the web sites which are accessed on school equipment.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported.

An incident log is used to monitor what is happening and identify trends or specific concerns.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the IT technician and an investigation by the Headteacher. This could possibly leading to disciplinary action, dismissal and involvement of police for very serious offences.

Protecting Personal, Sensitive, Confidential and Classified Information

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access.
- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- The security of any personal, sensitive, confidential and classified information contained in documents which are copied, scanned or printed.
- Only download personal data from systems if authorised to do so by the Headteacher.
- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
- Hard copies of data are securely stored and disposed of after use in accordance with the document labelling and GDPR compliance.
- They always protect school information and data, including any printed material.

Viruses

- All files downloaded from the internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- All users must never interfere with any anti-virus software installed on school IT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If it is suspected there could be a virus on any school IT equipment, the users must stop using the equipment and contact the IT technician who will contact the IT support provider immediately. The IT support provider will advise the school what actions to take and be responsible for advising others that need to know.

Disposal of IT Equipment

- All redundant IT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant IT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.
- All redundant IT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

Disposal of any IT equipment will conform to current legislation and will confirm with the governors' policy on the disposal of equipment.

Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- The IT technician will ensure that all user accounts are disabled once the member of the school has left the school.

Policy Reviewed: September 2024

Review Date: September 2025

Appendix A

E-Safety Agreement

At school we use the computers, iPads and the internet to help everybody with their learning. We follow the rules below to keep everyone safe.

- Follow the SMART rules

- Keep your personal information private
- Think about what you say and do online and treat people with respect
- Tell a trusted adult if you are worried about anything online
- Ask an adult if you can use a computer or an iPad if you are not in a computing lesson
- Only use the programmes that are appropriate for the lesson
- Ask permission before entering any website unless your teacher has already said you can use it
- Do not open unknown links and attachments
- Do not edit other children's files in Purple Mash

If you do not follow these rules then you could be stopped from using the internet, computers or iPads.

September 2024

Appendix B

ACCEPTABLE USE OF TECHNOLOGY (INCLUDING MOBILE PHONES) AGREEMENT

I understand that the school Internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the Internet and I am aware of the consequences if I breach them.

I am aware that by breaching the rules and regulations it may lead to:

- withdrawal of my user access;
- the monitoring of how I use the Internet;
- disciplinary action;
- criminal prosecution.

I will report immediately to the IT technician and Designated E-Safety Lead any accidental access to inappropriate material or websites that I may have.

I will log on to the internet by using my password, which will be changed if I think someone knows it.

When using the school's internet I will not:

- use the internet in such a way that it will bring the school into disrepute;
- use inappropriate or illegal websites;
- download inappropriate material or unapproved software;
- disrupt the time of other internet users by misusing the internet;
- use inappropriate language;
- use language that may provoke hatred against any ethnic, religious or other minority groups;
- produce, send out, exhibit or publish material that will cause offence to anyone;
- divulge any personal information about myself, any other user or that of pupils;
- divulge my login credentials or passwords to anyone;
- use the login credentials or passwords of any other user;
- use a computer that is logged on by another user;
- use any social networking site inappropriately but only to use it in order to develop teaching and learning;
- transfer the images of pupils without prior permission of the Headteacher and from parents;
- use email for private use but only for educational purposes;
- compromise the Data Protection Act (GDPR) or the law of copyright in any way.

I understand that during the school day I am restricted to using my mobile phone to break times and lunchtimes and that my mobile phone must be switched off during lesson/work times.

I agree to abide by the conditions in this policy:

Employee Name:		**Headteacher Name:**	
Employee Signature:		**Headteacher Signature:**	
Date:		**Date:**	