Cedar Park School

E-Safety Policy

Persons responsible for policy: Luke Redman

Date Written: March 2024

Date to be Reviewed: March 2025

Contents

1.0	Policy Aims	2
2.0	Policy Scope	2
3.0	Roles and Responsibilities	3
4.0	E-safety in the Curriculum	4
5.0	Training and engagement with staff	5
6.0	Awareness and engagement with parents and carers	6
7.0	Reducing Online Risks	6
8.0	Safer use of technology	6
9.0	Social Media	9
10.0	Use of Personal Devices and Mobile Phones	11
11.0	Responding to Online Safety Incidents and Concerns	12
12.0	Procedures for Responding to Specific Online Incidents or Concerns	13
13.0	13. The Use of AI in school	16
14.0	Useful Links for Educational Settings	16

1.0 Policy Aims

At Cedar Park we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies.

This policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2024, Early Years and Foundation Stage and 'Working Together to Safeguard Children' 2023. Please also refer to Cedar Park's AI policy in schools.
It also takes advice from the DfE on Teaching online safety in schools and Preventing and tackling bullying and cyber-bullying.

The purpose of this Cedar Park Primary School online safety policy is to:

- Safeguard and protect all members of the Cedar Park School community online
- Identify approaches to educate and raise awareness of online safety throughout the school community
- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

Cedar Park School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2.0 Policy Scope

Cedar Park School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.

Cedar Park School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.

Cedar Park School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as "staff" in this policy), as well as learners, parents and carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site (such as work laptops), tablets or mobile phones.
This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to the following school policies: computing, child protection, behaviour, health and safety, AI, anti-bullying and PHSE.

3.0 Roles and Responsibilities

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

The Designated Safeguarding Lead (DSL), Mr L Redman (Headteacher) has lead responsibility for online safety. Whilst activities of the Designated Safeguarding Lead may be delegated to an appropriately trained deputies Miss S Mason (Assistant Head), Mrs E Harper or Mrs J Collins, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. A link governor for e-Safety will be appointed by the FGB and this person will be responsible for holding the headteacher and e-Safety leader to account, as well as reporting back to the FGB.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The Designated Safeguarding Lead

Details of the school's DSL and deputy DSL are set out in our child protection policy as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs and the Computing Coordinator to ensure online safety is recognised as part of the setting's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Report online safety concerns, as appropriate, to the setting's management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually)
- Provide the Governing Body termly with current online safety information.

3.4 The ICT consultant

The ICT consultant role is provided by our ICT partner, Turn It On. They are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4.0 E-safety in the Curriculum

Cedar Park School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:

- Ensuring education regarding safe and responsible use precedes internet access
- Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and through computing programmes of study
- Supplementing e-safety learning within our Computing scheme with additional, explicit lessons from the Common Sense Education scheme of e-safety learning
- Reinforcing online safety messages whenever technology or the internet is in use

Pupils will be taught about online safety as part of the curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Consider the importance of a balance between online and offline activities
- Be aware and respectful of people while using devices
- 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** will be taught to:

- Use technology safely, respectfully and responsibly
- Consider the importance of a balance between online and offline activities
- Identify ways to keep information private online
- Recognise acceptable and unacceptable behaviour
- Be aware of the digital footprint they create online
- Identify a range of ways to report concerns about content and contact

By the **end of primary schoo**l, pupils will know:

- 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
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.0 Training and engagement with staff

Cedar Park School provide and discuss the online safety policy and procedures with all members of staff as part of induction including details on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails and staff meetings).

Through training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:

- Abusive, harassing, and misogynistic messages
- Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
- Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

6.0 Awareness and engagement with parents and carers

Cedar Park School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies. We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days. Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

7.0 Reducing Online Risks

Cedar Park School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. As a result, we will ensure that we carry out the following:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

However, due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

8.0 Safer use of technology

8.1 Technology within the classroom.

Cedar Park School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices such as tablets.
- The internet which may include search engines and educational websites and email.

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home. The setting will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.

Search engines are automatically set to safe search where possible. This reduces but does not eliminate the risk of links to inappropriate content and a filtering system is in place to ensure an additional level of safety.

We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.

Within Early Years Foundation Stage and Key Stage 1, access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners' age and ability.

Across Key Stage 2, learners will use age-appropriate search engines and online tools and will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

8.2 Managing Internet Access

All staff and learners will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

8.3 Filtering and Monitoring

- Cedar Park School governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks, including terrorist and extremist material. In order to ensure this, the school uses EXA SurfProtect system of filtering.
- The leadership team will ensure that regular communication takes place with our IT consultant and that checks are made to ensure that the filtering and monitoring methods are effective and appropriate and that content lists are regularly updated.
- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.
- All school devices should be connected to a filtered feed. If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content.
- Visitors can be given access to a Guest Wi-Fi network which, as well as being filtered and monitored, does not allow access to the school network.

- In the event of a learner discovering an unsuitable site, we are all trained in the following steps:

    - The learner turns off monitor/screen and immediately reports the concern to a member of staff.
    - The member of staff can remove and replace the device, ensuring learners are aware of risk where necessary.
    - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff. This can be done immediately via CPOMS.
    - The breach will be recorded on the filtering and monitoring spreadsheet tracker and escalated as appropriate. The DSL and DDSL have access to this sheet.
    - Parents/carers will be informed of filtering breaches involving their child.
    - Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Police or CEOP.

8.4 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation. Full information can be found in our Data Protection policy.

8.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems. This includes the following:

- Virus protection being updated regularly (managed by our IT consultant).
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- The appropriate use of user logins and passwords to access our network.
- All members of staff have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

8.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learners' personal information will not be published on our website or social media pages; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

8.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

8.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
- All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email.

Pupil email

- Pupils may use provided email accounts for educational purposes within computing lessons.
- Pupils will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

8.9 Educational use of Videoconferencing and/or Webcams

- Cedar Park School recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits and allows access to learning for those unable to attend the school setting.
- All videoconferencing and/or webcam equipment will be switched off when not in use and will not use auto-answer.
- Videoconferencing contact details will not be posted publicly.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- In the event that a recording of a videoconference lesson is required, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners

- Parents/carers consent will be obtained prior to pupils taking part in videoconferencing activities
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access

8.10 Management of Applications (apps) used to record children's progress

- EYFS currently use Tapestry to track learners progress and share appropriate information with parents and carers
- Staff have access to online assessment tools
- The Head teacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- In order to safeguard pupils' data:

    - Personal staff mobile phones or devices will NOT be used to access or upload content to any apps which record and store learners' personal details, attainment or images
    - 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
    - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

9.0 Social Media

9.1 Social Media Expectations

- The expectations regarding safe and responsible use of social media applies to all members of the Cedar Park School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messengers.
- All members of the Cedar Park School community are expected to engage in social media in a positive, safe and responsible manner.
- All members of the Cedar Park School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
- The use of social media during school hours for personal use is permitted during staff break times or with explicit permission by the Head teacher.
- Inappropriate or excessive use of social media during school hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member the Cedar Park School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

9.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.
- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
- Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):

    - Setting the privacy levels of their personal sites.
    - Being aware of location sharing services.

- Opting out of public listings on social networking sites.
- Logging out of accounts after use.
- Keeping passwords safe and confidential.
- Ensuring staff do not represent their personal views as that of the setting.

- Members of staff are encouraged not to identify themselves as employees of Cedar Park School on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.
- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles.
- Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Head teacher.
- If ongoing contact with pupils is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Head teacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL (or deputy).

9.3 Pupils Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources. Any concerns regarding pupils' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

Pupils will be advised:

- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications
- How to report concerns both within the setting and externally

9.4 Official Use of Social Media

- The Cedar Park School official social media channels are through Facebook, Instagram and Twitter.
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- The official use of social media as a communication tool has been formally risk assessed and approved by the Head teacher.
- The Head teacher has access to account information and login details for our social media channels.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
- Official social media sites are suitably protected and, where possible, run and linked to our website.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
- All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and pupils will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.

- Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
- Any official social media activity involving pupils will be moderated.
- Parents and carers will be informed of any official social media use with pupils; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

10.0 Use of Personal Devices and Mobile Phones

10.1 Staff Personal Use of Mobile Phones

Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.

Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time.
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
- Not connect mobile phones and personal devices to the school Wi-Fi as this poses a security risk to the school network.
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
- Not use personal devices during teaching periods, unless written permission has been given by the Head teacher such as in emergency circumstances.
- Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting pupils or parent/ carers. Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) or Head teacher.

Staff **will not** use personal devices:

- To take photos or videos of pupils and will only use work-provided equipment for this purpose.
- Directly with pupils and will only use work-provided equipment during lessons/educational activities.

If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour policy.
If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted.

10.2 Pupil Use of Mobile Phones

- Smart phones, smart watches and tablets are expressly prohibited from being on the school site and if found will be left in the front office and a parent will be asked to collect it at the end of the day. A "featurephone" (AKA a brick phone) is allowed on site in the year 6 class only and Cedar Park School expects pupils' personal devices and mobile phones to be handed to the class teacher and will be kept in a secure place, switched off and kept out of sight during lessons.
- If a pupil needs to contact his/her parents or carers they will be allowed to do so via the school office.
- Parents are advised to contact their child via the school office.
- If a pupil breaches the policy, the phone or device will be confiscated and will be held in a secure place. Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
- Searches of mobile phone or personal devices will only be carried out in accordance with our policy. https://www.gov.uk/government/publications/searching-screening-and-confiscation
- Pupils' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
- Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
- If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

10.3 Visitor Use of Mobile Phones

- Parents, visitors and volunteers (including governors and contractors) must adhere to this policy if they are on the school site during the school day.
  This means:
    - not taking pictures or recordings of pupils, unless it's a public event (such as a school fair) and with the authority of the headteacher
    - not using any photographs or recordings for personal use only, and not posting on social media without consent
    - not using phones in lessons, or when pupils are present
    - ensuring phones are on silent or vibrate while on the school grounds

- Parents, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at the School Office or attend a public event at school.
- Parents are permitted to take photographs at events such as sports day or performances with the headteacher's agreement. They are reminded that these should not under any circumstances be published on social media of any kind.
- Under no circumstances must parents use their phone (for calls, messages, photographs or internet) whilst in the school building. This extends to smart watches and cameras/recording equipment.
- Upon arriving at the school, visitors will confirm that they understand the rules around use of mobile phones in school.

- Parents or volunteers supervising school trips or residential visits must not:
    - Use their phone to contact other parents
    - Take photos or recordings of pupils, their work, or anything else which could identify a pupil

- Parents or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in this policy.
- Parents must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on his/her personal mobile during the school day Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Head teacher of any breaches our policy.

10.4 Officially Provided Mobile Phones

- Setting mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10.5 Loss, theft or damage

- The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.
- Parents and children will sign a home-school agreement explaining that the school accepts no responsibility for mobile phones as above.
- Confiscated phones will be stored securely in the school office
- Lost phones should be returned to the school office. The school will then attempt to contact the owner.

11.0 Responding to Online Safety Incidents and Concerns

- All members of the Cedar Park School community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
- Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and pupils to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- The school will follow the NSPCC guidance on when to contact the Police.

11.1 Concerns about Learners' Welfare

- **The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.**
- The DSL (or deputy) will record these issues in line with our child protection policy.

- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the DSCP thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

11.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Head teacher, in accordance with the safeguarding policy.
- Issues which do not meet the threshold requiring reporting to the LADO will be recorded in the school's record of low-level concerns.
- Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

12.0 Procedures for Responding to Specific Online Incidents or Concerns

12.1 Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" (2021) guidance and part 5 of 'Keeping children safe in education' 2024.
- Cedar Park School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
- Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- Cedar Park School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- Cedar Park School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- Cedar Park School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- **If made aware of online sexual violence and sexual harassment, we will**:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on pupil's electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as First Contact and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

12.2 Youth Produced Sexual Imagery

- Cedar Park School recognises youth produced sexual imagery (known as "nudes") as a safeguarding issue; **all concerns will be reported to and dealt with by the DSL** (or deputy).
- This section only applies to YP under the age of 18 creating/sharing/receiving nudes of a YP. It does not apply to children sharing adult pornography.
- On any occasion when an adult is in possession of or is sharing an illegal image of a YP – this will always be an urgent police matter.
- We will follow the advice set out by UKCIS here https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people a summary of the guidance.

- Cedar Park School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.
- We will review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

12.3 Online Child Sexual Abuse and Exploitation

- Cedar Park School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- Cedar Park School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, **all concerns will be reported to and dealt with by the DSL** (or deputy).
- Schools are reminded that a criminal offence has been committed if a person aged 18 or over intentionally communicates with a child under 16, who the adult does not reasonably believe to be 16 or over, if the communication is sexual or if it is intended to encourage the child to make a communication which is sexual. The offence will be committed whether or not the child communicates with the adult. This is the offence of sexual communication with a child under section 67 of the Serious Crime Act 2015
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community via our school's website.

  If made aware of incident involving online child sexual abuse and we will:

  - Act in accordance with our child protection policies and procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to First Contact (if required/appropriate) and immediately inform police via 101, or 999 if a child is at immediate risk.
  - Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.

- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via CEOP: www.ceop.police.uk/safety-centre
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the LEA or via the Police.

12.4 Indecent Images of Children (IIOC)

- Cedar Park School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately from the Police and/or the Education Safeguarding Team. **If made aware of IIOC, we will:**

    - Act in accordance with our child protection policy and the relevant procedures.
    - Store any devices involved securely.
    - Immediately inform appropriate organisations, such as CEOP, Police or the LADO.

- **If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will**:

    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
    - Ensure that any copies that exist of the image, for example in emails, are deleted.
    - Report concerns, as appropriate to parents and carers.

- **If made aware that indecent images of children have been found on the setting provided devices, we will:**

    - Ensure that the DSL (or deputy) is informed.
    - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
    - Ensure that any copies that exist of the image, for example, in emails, are deleted.
    - Inform the Police via 101 (999 if there is an immediate risk of harm) and First Contact
    - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the Police.
    - Report concerns, as appropriate to parents and carers.

- **If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will**:

    - Ensure that the Head teacher is informed in line with our managing allegations against staff policy.
    - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
    - Quarantine any devices until police advice has been sought.

12.5 Child Criminal Exploitation – Including County Lines

- All staff need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in the schools safeguarding policy.

12.6 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at Cedar Park School.
- 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 them 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 the victim.
- The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their year groups.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes e-safety lessons, personal, social, health and economic (PSHE) education, and other subjects where appropriate.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

12.7 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Cedar Park School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the Cedar Park community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through First Contact or from the Police.

12.8 Online Radicalisation

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Head teacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

13.0 13. The Use of AI in school

This applies to all students, staff, volunteers, and visitors who may use AI-based tools and resources within the school environment, both on school premises and during remote learning.

AI platforms must be approved by the school's Headteacher (which may be delegated to the IT subject lead) and follow strict data security protocols to protect student and staff information. Regular audits will be conducted to ensure data is stored, processed, and deleted in accordance with school policies.

- Teachers: Ensure responsible use of AI tools, integrating them into lessons in a way that enhances learning. Ensure AI tools are developmentally appropriate and maintain oversight.
- School Leadership: Provide guidance on policy adherence and encourage the development of AI literacy among students and staff.
- Students must use AI responsibly and ethically, under the guidance of teachers.
- Understand the limits of AI and the importance of developing critical thinking skills alongside technology use.
- Parents/Guardians should stay informed about AI tools used in the school and provide consent where required.

See Cedar Park's AI policy for further information and full consideration when adopting AI practice in and out of the classroom.

14.0 Useful Links for Educational Settings

- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- Parent Protect https://www.parentsprotect.co.uk - this includes advice for parents on peer on peer abuse and how to cope if your child has got into significant trouble online.
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Parentzone (Google Internet Legends) https://parentzone.org.uk/

Appendix 1: Model acceptable use of the internet: agreement for parents and carers



Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

Our official Facebook, Instagram and X accounts

Email/text groups for parents (for school announcements and information)

Our website

Tapestry (EYFS only)

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp)

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook Twitter accounts, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's Facebook / Twitter accounts, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:	**Date:**

Appendix 2: Acceptable use agreement for KS2 pupils

	Cedar Park School **Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers**
Name of pupil:	

I will read and follow the rules in the acceptable use agreement policy

When I use the school's ICT systems (like computers and equipment) and get onto the internet in school

I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Use AI responsibly and ethically, under the guidance of teachers. I must understand the limits of AI and the importance of developing critical thinking skills alongside technology use.

I will not:

- Access any inappropriate websites including, but not limited to: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of learning
- If using email, open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision
- Break school rules, or conduct any inappropriate behaviour
- Engage in disrespectful behaviour towards others when online
- Use AI to plagiarise work that will be submitted under the guise of my own work.
- I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I understand that the school can discipline me if I break the rules, even if I'm not in school when I do this

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Appendix 3: Acceptable use agreement for staff, governors and volunteers

Cedar Park School
Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors and volunteers

E-safety Responsibilities

I am aware that the Headteacher (DSL) has overall responsibility for e-safety at Cedar Park
Additional responsibility for e-safety (online safety) is shared with deputy DSLs: Miss S Mason (Assistant Head), Mrs E Harper and Mrs J Collins.

Photographs and Video

- I will always use a school camera to capture images.
- If I am sharing photos/videos online, then I will ensure the names of pupils are not be linked to pupil photos
- If sharing photos/videos online, I will first make sure I am fully aware of the consent form responses from parents

Security and passwords

- I will set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- I will 'lock' the PC if leaving it unattended.
- I will not install any unauthorised software, or connect unauthorised hardware or devices to the network

Data storage

- I will only use encrypted USB drives in school.
- I will risk assess any data that I plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact.

Reducing risk

- I will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

Reporting issues

- **I will report all breaches of the e-safety policy using CPOMS or (if this is not possibly) directly to a DSL who will report this on CPOMS on my behalf**
- I will report any allegations involving staff to the Headteacher.
- I will report any allegation against the Headteacher to the Chair of Governors.
- I will keep evidence of incidents.

Managing Email

- I will not forward of any chain messages/emails
- I will report and block spam or junk mail
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email or using documents that are password protected.
- I will immediately tell the DSL if I receive offensive communication, and this will be recorded in our safeguarding files/records.
- I will not use my personal email addresses any official setting business.

Visiting sites

- I will not visit internet sites via the school network and make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornography (including child pornography).
    - Promoting discrimination of any kind.
    - Promoting violence or bullying.
    - Promoting racial or religious hatred.
    - Promoting illegal acts.
    - Breach any Local Authority/School policies, e.g. gambling.

Cont. on next page

Use of AI in and outside of the classroom

Ensure responsible use of AI tools, integrating them into lessons and administrative reports in a way that enhances learning and/or administration of the school's effectiveness. Ensure AI tools are developmentally appropriate and maintain oversight in a classroom based setting. I will not share children's information on a third party AI site.
School Leadership: Provide guidance on policy adherence and encourage the development of AI literacy among students and staff.

Mobile phones

- I will keep my mobile phone secure and on silent
- I will not connect my mobile phone or personal device to the school Wi-Fi
- I will not use personal devices during teaching periods, unless permission has been given by the Head teacher such as in emergency circumstances.
- I will not use my personal phones or devices for contacting pupils or parent/carers unless permission has been given by the Head teacher such as in emergency circumstances. In this situation I will use 141 to hide my caller ID.
- I will not take photos or videos of pupils on my own device and will only use work-provided equipment for this purpose.

Communication

I will only communicate with pupils and parents through official channels when discussing school/business related topics.

I am aware that the ICT system is filtered and monitored.

I am aware that civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

I agree to return school IT equipment to the school without delay at the request of the Computing Lead or School Senior Leadership Team.

Signed:	**Date:**

Appendix 4: Template mobile phone information for visitors

	Cedar Park School **Mobile phone information for parent, visitors and volunteers**

Parents, visitors and volunteers (including governors and contractors) must adhere to the guidelines stated in this document if they are on the school site during the school day.

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present
- Please do not use mobile phones (for calls, messages, photographs or internet) whilst in the school building. This extends to smart watches and cameras/recording equipment
- Please do not take photos or recordings of pupils (unless it is your own child), or staff
- Any photographs or recordings must be for personal use only, and cannot be shared on social media
- Do not use your phone in lessons, or when working with pupils

Parents or carers are permitted to take photographs of their child at events such as sports day or performances with the headteacher's agreement. They are reminded that these should not under any circumstances be published on social media of any kind.

Please be aware that the school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips.

Lost phones that are discovered on site will be returned to the school office. The school will then attempt to contact the owner.

A full copy of our e-safety policy is available from the school office.

Signed (governor/volunteer/visitor):	**Date:**

Appendix 5: **online safety training needs – self audit for staff**

	Cedar Park School **Online safety training audit**
Name of staff member/volunteer:	
Date:	

Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the different ways in which pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 6: **Response Flowchart**

