Chase Lane
Primary School and Nursery

E-SAFETY POLICY

Our school promotes perseverance, resilience and mutual respect. Working in partnership with families, we ensure that all children are given the best opportunities throughout their educational journey. Children at Chase Lane embrace challenge and make the best possible progress to enhance their life choices in an ever changing, diverse modern Britain.

January 2024

Title: E-Safety Policy

Function: Information and Reference

Subject Category: Safeguarding

Audience: All staff, Parents, Pupils and Governors

Date of Review: January 2025

Member of Staff Responsible: Headteacher and SLT

This policy should be read in conjunction with:

Acceptable Personal Use of Resources and Assets Policy

Appendix 1 - ICT Acceptable Use Policy - Code of Conduct Policy

Aims

The aims of this policy are:

- To educate and encourage pupils to access technology safely
- To prevent the risks arising from
  (i) exposure to illegal, harmful or inappropriate content
  (ii) the sharing of personal data, including images
  (iii) inappropriate online contact or conduct
  (iv) cyberbullying and other forms of abuse

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-safety incidents and monitoring reports. The Governor responsible for Safeguarding also monitors the effectiveness of the school's E-safety Policy.

The role of the Safe-guarding Governor will include:

- Regular meeting with the E-Safety Co-ordinator (Headteacher)
- Regular monitoring of E-safety incident logs
- Reporting to relevant committee meetings

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including E-safety) of members of the school community.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious E-safety allegation being made against a member of staff, including how to contact the LADO.
- The Headteacher is responsible for ensuring that relevant staff receive suitable training to enable them to carry out their E-safety roles and to train other colleagues, as relevant.

- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive reports of any incidents.
- The Headteacher takes day to day responsibility for E-safety issues and has a leading role in establishing and reviewing the school E-safety policies / documents
- The Headteacher ensures that all staff are aware of the procedures that need to be followed in the event of an E-safety incident taking place.
- The Headteacher provides training and advice for staff
- The Headteacher liaises with school technical staff
- The Headteacher receives reports of E-safety incidents and creates a log of incidents to inform future E-safety developments,
- meets regularly with Safeguarding Governor to discuss issues and review incident logs

IT Technician:

The IT Technician is responsible for ensuring that:

- the school has an effective anti-virus programme in place
- the school meets the E-Safety technical requirements outlined in the E-Safety Policy
- they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant
- monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:
Are responsible for ensuring that:

- they have an up to date awareness of E-safety matters and of the current school E-safety policy and practices, including the DfE Filtering and Monitoring Standards
- they have read and understood the Code of Conduct Appendix 1 – ICT Acceptable Use Policy and Acceptable Personal Use of Resources and Assets policy (C5)
- they report any suspected misuse or problem to the Headteacher for investigation

- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-Safety Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- pupils are taught about staying safe online, both in and outside of school
- there are ongoing conversations with pupils about the benefits and dangers of the internet and there is an open environment for pupils to ask questions and raise any concerns

Child Protection / Safeguarding Designated Lead:

The DSL is trained in E-safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the *school* digital technology systems in accordance with the E-Safety Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents / carers do not fully understand the issues and are less experienced in the use of digital technology systems than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature.

Parents and carers will be encouraged to support the school in promoting good E-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- their children's personal devices in the school (where this is allowed)

Policy Statement

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in E-safety is therefore an essential part of the school's E-safety provision. Children need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce E-safety messages across the curriculum. The E-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models (in line with the school's code of conduct) in their use of digital technologies, the internet and mobile devices
- Where pupils are allowed to search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Misuse

Any misuse of technology by pupils at Chase Lane Primary School and Nursery will be dealt with under the school's Behaviour and Relationships Policy and, where safeguarding concerns are raised, under the Child Protection Policy and procedures.

Children will be taught that they must not use their own or the school's technology to bully others whether during school or outside of school hours. Bullying incidents involving the use of technology, including cyberbullying will be dealt with under the school's Anti-bullying Policy. If a child thinks they have been bullied or that another child is being bullied, they should talk to a known adult about it as soon as possible.

If a pupil is worried about something that they have seen on the internet or on any electronic device, including on another person's electronic device they must inform a known adult as soon as possible.

Education & Training – Staff / Volunteers

It is essential that all staff receive E-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal E-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the E-safety training needs of all staff will be carried out regularly.
- All new staff should receive E-safety training as part of their induction programme, ensuring that they fully understand the school E-safety policy and Acceptable Use Agreements.
- The Headteacher will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Headteacher will provide advice / guidance / training to individuals as required.

Training – Governors

Governors take part in E-safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / E-safety / health and safety / child protection. This is offered in a number of ways:

- Attendance at training provided by the Local Authority or other relevant organisation.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets the DfE Filtering and Monitoring Standards for Schools and Colleges (March 2023)
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

- All users will have clearly defined access rights to school digital technology systems and devices.
- All users will be provided with a username and secure password. Users are responsible for the security of their username and password.
- The “master / administrator” passwords for the school digital technology system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe).
- IT Technician is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

Pupils may use individual or class log-ons to access the network where appropriate.

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreement is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems.
- An agreement is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreement is in place that forbids staff, unless approved by the administrator, from downloading executable files and installing programmes on school devices

Internet access is filtered for all users.

- An agreement is in place regarding the use of removable media (e.g. memory sticks) by users on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

See Appendix 1 - Acceptable Use Policy – Code of Conduct

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place.

Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils and staff must not take, use, share, publish or distribute images of others without their permission or their parents / carers.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website as part of the agreement signed by parents when a child joins the school.

Data Protection

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

- All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.
- It has a Data Protection Policy
- It is registered as a Data Controller
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat, etc.) must be professional in tone and content where school matters are concerned.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the *school* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the Data Protection and Appendix 1 – ICT Acceptable Use Policy

Use of mobile electronic devices and smart technology

Children are allowed to bring mobile phones to and from school to ensure their personal safety.

Children must not use a mobile device, smart watch or electronic device including headphones anywhere in school during the school day, except under the specific direction of a teacher.

Rules for Responsible Internet Use by Pupils

The school has Internet access and access to digital technologies to help our learning. In return, we will agree to these rules to keep everyone safe and help us be fair to others.

- I will use only my own login and password and I will not share it.
- I will only access the Internet with the permission and supervision of a member of staff
- I will not access, copy, or delete other people's files.
- I will only use computers and digital devices for schoolwork and homework.
- I will not bring USB drives or other removable storage media into school without permission.
- I will not try to download programmes or apps or upload content to the internet without permission.
- I will only email or message people my teacher has approved and any messages / chats will be friendly, polite, and sensible.
- I will not copy other people's work, unless I have permission.
- I will not share my personal information, or that of my friends, including sharing photos/images without permission or arrange to meet someone online.
- To help protect other pupils and myself, I will tell a teacher if there is anything I am unhappy with or if I see a computer warning.
- I will ask for help if I am not sure what to do.
- I understand that the school can check my computer files and the Internet sites I visit.
- I will not download programs, apps, or files to school devices from the Internet.
- I will not print, unless it is related to my work.
- I will take care of the devices and equipment I use and I will treat them with respect.

Name of child: _____

Signed by _____ (Child)

Parent/Carer

I have read through the acceptable use agreement with my child and explained what is expected of them.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure young people are safe when using the internet and digital technology.

I understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using digital technologies.

I will encourage my child to seek help and support if they raise concerns about the online world and I will inform school if I have any online safety concerns.

I understand that my child's activity on school systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement

Signed: _____ (Parent/Responsible Adult)