Online Safety Policy

Agreed by Local Governing Body: 20th May 2019

This policy sits under and should be read in conjunction with The Elliot Foundations' Online Safety Policy.

The term 'e-safety' has been replaced with 'Online Safety' inline with the Common Inspection Framework 2015 to reflect issues that go beyond the scope of safeguarding.

Other documents that are useful in conjunction with this policy are:

Safeguarding in early years, education and skills settings, Ofsted, Updated 2018; www.gov.uk/government/publications/inspecting-safeguarding-in-early-years-education-and-skills-from-september-2015.

Keeping children safe in education, Department for Education, Updated September 2018; www.gov.uk/government/publications/keeping-children-safe-in-education--2

Working together to safeguard children, Department for Education, March 2015; www.gov.uk/government/publications/working-together-to-safeguard-children--2.

This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place outside of the school , but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Online safety in schools is a child safety and not an ICT issue. Therefore this policy should be viewed alongside other Safeguarding policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship.

Rationale

At Cavalry Primary School we believe that the use of information and communication technologies in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively and safely.
The use of these exciting and innovative technology tools in school and at home has been shown to raise educational standards and promote pupil achievement. Yet at the same time we recognise that the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning
- Inappropriate use of social media

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our

children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Technology in our school

The school's ICT infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.

Ref: E2BN Website

In December 2019 we will transfer from the current provider to Eastnet. This is a service that will continue to be provided by Cambridge County Council and will see continue to provide at least the current level of protection offered. Further news on this transfer can be found here:
https://www.cambridgeshire.gov.uk/news/mll-telecom-named-eastnet-managed-network-services-provider/

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and Online safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Technologies regularly used by pupils and adult stakeholders include:
Staff:
Laptops, tablets, chromebooks and desktops
Cameras and video cameras
Internet, E-mail, Google drive, G-suite, MIS (Scholar Pack), Parentpay and confidential pupil information

Pupils:
Laptops, desktops, chromebooks and tablets
Cameras and video cameras,
Internet, Google drive, G-suite, Accelerated Reader, Mathletics, Google classroom and other communication tools
Other peripherals such as programmable toys, data loggers, control technology equipment

Nursery:

staff laptop
Desktops, Laptops, tablets used by children
cameras used by staff and children
staff use of internet and email - G-suite and Google Drive

We are currently in the process of migrating to individual logins (as recommended by OFSTED) across the school.
All members of staff have individual, password protected logins to the school network. The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office. Visitors may be connected to the network by SLT, but the wireless Key must not be shared. Connection to the Wireless network will provide internet access, but will not allow them access to confidential systems which are protected by other passwords and logins.

Use of handheld technology (USB, personal phones and handheld devices)
We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:
The use of USB sticks and external hard drives are not permitted in school unless approved by SLT for a specific activity (the electric piano, restoring software to laptops). They must not be used to transfer confidential data.
Members of staff are permitted to bring their personal mobile devices into school. They are required to use these in accordance with the Mobile Phone Policy

GDPR

In order to be fully GDPR compliant, all online user accounts will be managed through the school MIS. Using an Identity Management service (RM Unify) all accounts can be monitored and managed by the IT Lead and Manager. This will ensure that;

All staff and students that leave the school will have their accounts suspended
All student accounts will be managed through one system
All students and staff will be provided with individual accounts (in the process of migrating to this)

Roles and Responsibilities

Governing Body

The governing body is accountable for ensuring that out school has effective policies and procedures in place, as such they will:

- Review this policy at least every three years and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing these incidents.
- Appoint one governor (????) who has overall responsibility for the governance of online safety at the school who will:
    - Keep up to date with the emerging risks and threats through technology use
    - Receive regular updates from the head teacher in regards to training, identified risks and any incidents.
    - Meet with the Online Safety Lead
    - Report to governors on online safety issues that arise

Head teacher and Senior Leaders

Reporting to the governing body, the head teacher has overall responsibility for online safety within our school.

The day to day management of this will be delegated to a member of staff, the online safety lead, as indicated below.

The Head teacher will ensure that:

- Online safety training throughout the school is planned and up to date and appropriate to the recipient, e.g. students, all staff, SLT and governing body, parents.
- The designated online safety lead has had appropriate CPD in order to undertake the day to day duties. The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- All online safety incidents are dealt with promptly and appropriately. The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on
- dealing with online safety incidents later in this policy). The Senior Leadership Team / Senior Management Team will receive regular monitoring reports from the

- Online safety Coordinator / Officer.

Online safety Lead

- The day to day duty of online safety officer is devolved to: ????

The online safety officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/ herself with the latest research and available resources for school and home use.
- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing this policy regularly along with other related document and bring any matters to the attention of the Head teacher.
- Advise the Head teacher, governing body on all online safety matters.
- Meet with the online safety governor regularly to discuss current issues, review incident logs and filtering / change control logs
- Provides training and advice for staff and ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Engage with parents and the school community on online safety matters at school and/or home.
- Liaise with the local authority/ TEFAT/RM IT technical support and other agencies as required.
- Ensure any technical online safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA/TEFAT/RM and ICT technical support.
- Make him/ herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function, liaise with the Head teacher and responsible governor to decide on what reports may be appropriate for viewing.
- Report regularly to the Senior Leadership Team and in partnership with them decides on the investigation/action and sanctions process for any online safety incidents.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit for purpose, up to date and applied to all capable devices.
    - Windows (or other operating systems) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as internet filtering are operating correctly.

    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and the Head teacher.
    - Passwords may not be applied to shared pupil areas. Passwords for staff will be a minimum of 8 characters.

- The school meets required online safety technical requirements and any Local Authority / other relevant body Online safety Policy / Guidance that may apply.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet/ email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and/ or Online safety Lead for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school / academy policies.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the head teacher or online safety officer.
- They have an up to date awareness of online safety matters and the current school policy and practices.
- They have read, understood, signed and abide by the acceptable use policy.
- All digital communication with pupils and parents/ carers should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other activities and implement current policies with regard to the use of digital technologies, mobile devices, cameras etc in lessons.
- Pupils understand and follow the online safety and acceptable use policies and have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- In lessons where internet use is pre-planned students / 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.
- Any online safety incident is to be reported to the online safety lead, and/ or the head teacher and recorded in Scholarpack.

The reporting flow charts contained within this online safety policy are to be understood.

Senior Designated Person for Safeguarding
Should be trained in online safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

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

Education - All 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 online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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

• A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

• Key online safety messages should be reinforced as part of a planned programme of assemblies

• Pupils should be taught in all lessons to be critically aware of the materials / content they access online 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 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 their use of digital technologies the internet and mobile devices

• In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

The boundaries of use of the ICT equipment and services in this school are given in the student acceptable use policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance to the behaviour policy.

The school has published Acceptable Use Policies for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Any known or suspicious online misuse or problem will be reported to the headteacher for investigation/ action/ sanctions.

Responding to Incidents – (Education Child Protection Service – June 2010)
It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to online safety incidents are consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
If an online safety incident occurs, Cavalry Primary School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (for ICT, this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix). Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed.

Dealing with Incidents and Seeking Help
If a concern is raised, refer immediately to one of the designated person for child protection. If that is not possible refer to another member of the Leadership Team or, if necessary, the Chair of Governors.
It is their responsibility to:
Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator
Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.
Step 3: Ensure that the incident is documented using the standard child protection incident logging form
Depending on the judgements made at steps 1 and 2 the following actions should be taken:
Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.
Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service
Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff.

Cavalry School's Offer to all children to support online safety

Every year we will:

- Hold an online safety week in the Spring Term to provide a focus for the whole school
- Include references to cyber-bullying in our Anti-Bullying activities each November
- Provide useful information/links to parents via the school website
- Raise awareness of online safety with regular updates in school newsletters
- Explicitly teach strategies for keeping safe in the digital world through PSHE units provided by Cambridgeshire PSHE Service every year from Y1 to Y6. We will keep parents informed about key messages from this teaching through curriculum newsletters.
- ACE accredited scheme for pupils in KS2
- Have a commitment to staff training, so that all staff are aware of school procedures, key safety messages and are kept up to date with technological developments
- Issue guidance to staff about social networking and blogs through the Staff Handbook

Terms used in this policy

AUP: Acceptable Use Policy.
A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse.
Child: Where we use the term 'child' (or its derivatives), we mean 'child or young person'; that is anyone who has not yet reached their eighteenth birthday.
Online safety: We use online safety, and related terms such as 'online', 'communication technologies', and 'digital technologies' to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose online safety risks. We try to avoid using the term 'ICT' when talking about online safety as this implies that it is a technical issue – which is not the case. The primary focus of online safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting online safety risks based on a combined approach to Policies, Infrastructure and Education, underpinned by Standards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for the school's approach to online safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. online safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of Every Child Matters: Change for Children. Those with responsibility for the development and delivery of online safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.