Greenvale Primary School

E-SAFETY AND COMPUTING POLICY

Policy Date	June 2021
Signed by Head Teacher	Mrs A Allnutt
Review Date	June 2022

Greenvale Primary School

E-Safety and Computing Policy

Policy Owner – Mrs Amanda Allnutt, Head Teacher and Mrs Sarah Wilder, Class Teacher

Policy Date – June 2021

Review Date – June 2022

Section 1- Monitoring

1.1 The Head Teacher will monitor the application of this policy and take appropriate steps to ensure that it is operating effectively.

1.2 The policy will be reviewed annually to ensure its effective application.

1.3 This policy is consistent with the schools' General Data Protection Regulation (GDPR) Policy

1.4 Linked Policies

1.4.1 General Data Protection (GDPR) Policy

1.4.2 Acceptable Use of ICT Policy

1.4.3 Behaviour for Learning Policy

1.4.4 Staff Use of Computers Policy

1.4.5 Cameras, iPads and Mobile Devices in EYFS & KS1 Policy

1.4.6 Safeguarding and child protection policy 2020

Section 2 - Policy Statement

2.1 For clarity, the E-safety safety policy uses the following terms unless otherwise stated:

- Stakeholders – Refers to staff, Governing Body, school volunteers, students and any other person working on behalf of the school including supply teachers and contractors.
- Parents – Any adult with a legal responsibility for a child or young person e.g. parent, carer, guardian.
- School – Any school business or activity conducted on or off the school site e.g. visits, conferences, school trips, etc.
- Wider School Community – Students, all staff and Governing Body.

2.2 Safeguarding is a serious matter. At Greenvale Primary School we use technology and the internet extensively across all areas of the curriculum.

2.3 E-safety safeguarding, known as internet safety is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis or in response to an e-safety safety incident, whichever is sooner.

2.4 The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk-free is met.

- To ensure risks are identified, assessed and mitigated, where possible, in order to reduce any foreseeability of harm to the student or liability to the school.

2.5 This policy is available for anyone to read on the Greenvale Primary School website (www.greenvale.medway.sch.uk); upon review all members of staff will sign to say that they have read and understand both the e-safety safety and Staff Acceptable Use Policy.

2.6 A copy of this policy and the Students Acceptable Use policy will be included in the admissions pack for parents to read, sign and return a copy to keep in the pupil file. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology, including the internet.

Section 3 - Policy Governance (Roles and Responsibilities)

Note: in this section you should note the roles and responsibilities of each person/body. Many schools will differ (e.g. Secondary and Primary) so it is important that this is discussed between the Head Teacher and Governing Body.

3.1 Governing Body - The Governing Body is accountable for ensuring that Greenvale Primary school has effective policies and procedures in place and they will:

- Review this policy at least annually and in response to any e-safety safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure e-safety safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one Governor to have overall responsibility for the governance of e-safety safety at the school who will:
  i. Keep up to fate with emerging risks and threats through technology use.
  ii. Receive regular updates from the Head Teacher in regards to training, identified risks and any incidents.
  iii. Chair the e-safety safety committee.

3.2 Head Teacher - Reporting to the Governing Body, the Head Teacher has overall responsibility for e-safety safety within our school. The day-to-day management of this will be delegated to a member of staff, the e-safety safety Officer (or more than one). The Head Teacher will ensure that:

- E-safety safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, Senior Leadership Team (SLT), Governing Body and parents/carers.
- The designated e-safety safety Officer(s) had had appropriate CPD in order to undertake the day to day duties.
- All e-safety safety incidents are dealt with promptly and appropriately.

3.3 The E-Safety Safety Officer - The day to day duty of the E-safety safety Officer is devolved to Mrs Sarah Wilder and will:

- Keep up to date with the latest risks to children whilst using technology; familiarize herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Head Teacher.
- Advise the Head teacher and Governing Body on all e-safety safety matters.
- Engage with parents and the school community on e-safety safety matters at school and/or at home.
- Liaise with the Local Authority (LA), ICT Technical Support and other agencies as required.
- Retain responsibility for the E-safety safety incident log; ensure that staff know what to report and ensure the appropriate audit trail.

- Ensure any technical E-safety safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose through liaison with the LA and/or ICT Technical Support.
- Make herself aware of any reporting function with technical E-safety 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.

3.4 ICT Technical Support Staff - ICT Technical Support staff are responsible for ensuring that the IT technical infrastructure is secure; this will include (at a minimum):

- Anti-virus software is fit for purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updates as appropriate.
- Any E-safety 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 E-safety safety Officer and Head Teacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters; passwords for students will be class-set.
- The IT System Administrator password is to be changed on a six monthly basis.

3.5 All Staff

- The E-safety safety policy will be formally provided to and discussed with all members of staff.
- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Head Teacher.
- Any E-safety safety incident is reported to the E-safety safety Officer (and an E-safety safety report is made), or in her absence to the Head Teacher to make a decision.
- The reporting flow charts contained within this E-safety safety policy are fully understood.
- All data created using the schools technology/services belongs to the school i.e. Videos, MLE, e-mails, forums, blogs, educational accounts for Apple/Amazon/Licencing…therefore it can be accessed by the head teacher at any time for auditing or safeguarding purposes

3.6 All Students - The boundaries of use of ICT equipment and services in this school are given in the Student Acceptable Use of ICT Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour for Learning Policy. E-safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be made fully aware of how they can report areas of concern whilst at school or outside of school. School council to be involved in the E-safety safety policy

3.7 Parents and Carers - Parents play the most important role in the development of their children; as such the school will ensure that parents and carers have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters, E-safety safety leaflets and school prospectus the school will endeavour to keep parents and carers up to date with new and emerging E-safety safety risks, and will involve parents and carers in strategies to ensure that students are empowered. Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents and carers will sign the Student Acceptable Use policy before any child can be granted access can be granted to school ICT equipment or services.

Section 4 - Technology

4.1 Greenvale Primary School uses a range of devices including PC's, ipads, learn pads and laptops.

4.2 In order to safeguard the student and in order to prevent loss of personal data, we employ the following assistive technology:

- Internet Filtering – We use software that prevents unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in-line with this policy or in response to an incident, whichever is sooner. The ICT coordinator, E-safety safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher.
- Email Filtering – We use software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as "an email that contains a virus or script (i.e. Malware) that could be damaging or destructive to data; spam email such as a phishing message."
- Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Head Teacher immediately. The Head Teacher will liaise with the LA to ascertain whether a report needs to be made to the Information Commisioners Office. *Note: encryption does **not** mean password protected).*
- Passwords – All staff and students will be unable to access any device without a unique username and password. Staff passwords will change on a six monthly basis or if there has been a compromise, whichever is sooner. The ICT coordinator and IT support will be responsible for ensuring that passwords are changed.
- Anti-Virus – All capable devices will have anti-virus software installed. The software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Head Teacher if there are any concerns. All USB peripherals such as keydrives are to be scanned for viruses before use.

Section 5 - Safe Use

5.1 Internet – Use of internet in school is a privilege, not a right. Internet use will be granted to staff upon signing this E-safety safety policy and the Staff Use of Computers Policy and to children after parental consent is obtained and they have returned the Acceptable Use of ICT Policy.

5.2 Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

5.3 Photos and Videos – Digital media such as photos and videos are covered in the school's Cameras, iPads and Mobile Devices in EYFS & KS1 Policy, and is re-iterated here for clarity. All parents and carers must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

5.4 Social Networking – There are many social networking services available. Greenvale Primary School is fully supportive of social networking as a tool to engage and collaborate with learners and to engage with parents and the wider community. The following social media services are permitted for use within Greenvale Primary school and have been appropriately risk assessed; should staff wish to use other social

media, permission must first be sought via the E-safety safety Officer who will advise the Head Teacher for a decision to be made. Any new service will be risk assessed before use is permitted.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video or any child is uploaded.
- There is to be no identification of pupils using their first name and surname
- All posted data must conform to Copyright Law; images, videos and other resources that are not originated by the school are not allowed unless the owners' permission has been granted or there is a licence which allows for such use.

5.5 Notice and Take Down Policy – Should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have Copyright Permission to use that resource, it will be removed within one working day.

5.6 Incidents – Any E-safety safety incident is to be brought to the immediate attention of the E-safety safety Officer, or in his/her absence the Head Teacher. The E-safety safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out the incident log.

5.7 Training & Curriculum – It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk-free as possible which using digital technology; this includes updated awareness of new and emerging issues. As such, Greenvale Primary School will have an annual programme of training which is suitable to the audience. E-safety safety for pupils is embedded into the Curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology, and risks as part of the pupil's learning. As well as the programme of training, we will establish further training lessons as necessary in response to any incidents. The E-safety safety Officer is responsible for recommending a programme of training and awareness for the school year to the Head Teacher and responsible for Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Head Teacher for further CPD. The E-safety safety training programme can be found in the school office.

5.8 Learning Platforms & Learning Environments –

- Children and staff will be advised on acceptable conduct and use when using the Learning Platform (LP)
- Only members of the current school, parents/carers and staff community will have access to the LP.
- All users will be mindful of Copyright issues and will only upload appropriate content onto the LP.
- When staff, children etc., leave the school, their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways:
    i. The user will be asked to remove any material deemed to be inappropriate or offensive.
    ii. The material will be removed by the site administrator if the user does not comply.
    iii. Access to the LP for the user may be suspended.
    iv. The user will need to discuss the issues with a member of the SLT before reinstatement.
    v. A pupil's parent/carer may be informed.
    vi. Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

Section 6 - E-safety safety Contacts and References

CEOP

Child Exploitation and E-safety Protection Centre

Website: www.ceop.police.uk

E-safety Safety Officer

The E-safety safety Officer is Rebecca Avery

Children Safeguard Team, Families and Social Care, Kent County Council

Email: esafetyofficer@kent.gov.uk

Telephone: 01622 221469

Childline

Telephone: 0800 1111

Website: www.childline.org.uk

Childnet

Website: www.childnet.com

Children's Officer for Training & Development

The Children's Officer for Training & Development is Mike O'Connell

Children Safeguard Team, Families and Social Care, Kent County Council

Email: mike.oconnell@kent.gov.uk

Telephone: 01622 696677

Children's Safeguard Team

Website: www.kenttrustweb.org.uk?safeguards

Clever Click Safe Campaign

Website: http://clickcleverclicksafe.directgov.uk

Cybermentors

Website: www.cybermentors.org.uk

Digizen

Website: www.digizen.org.uk

EiS

ICT Support for school's and ICT security advice

Website: www.eiskent.co.uk

Telephone: 0300 0658888

Internet Watch Foundation (IWF)

Website: www.iwf.org.uk

Keeping children safe in Education 2020 – Annex C: online safety
Website: www.KCSIE2020

Kent E-safety safety in School's Guidance
Includes a school audit tool and notes on the legal framework as part of the PDF versions of this document),
Website: www.kenttrustweb.org.uk?safety

Kent Police
In an emergency, a life is in danger or a crime process **dial 999.**
For other non-urgent enquiries contact Kent Police on:
Telephone: 01622 690690
Website: www.kent.police.uk or www.kent .polic.uk/internetsafety

Kent Public Services Network (KPSN)
Website: www.kpsn.net

Kent Safeguarding Children Board (KSCB)
Website: www.kscb.org.uk

Kidsmart
Website: www.kidsmart.org.uk

School's Broadband Service Desk
Help with filtering and network security.
Website: www.eiskent.co.uk
Telephone: 01622 206040

School's E-safety safety Blog
Website: www.kenttrustweb.org.uk?esafetyblog

Search engine
www.kiddle.co/

Teach Today
Website: http://en.teachtoday.eu
Think U Know
Website: www.thinkuknow.co.uk
Virtual Global Taskforce
Report abuse to:
Website: www.virtualglobaltaskforce.com

APPENDIX A – Password Security poster