E-safety Policy

This policy covers all pupils in the school, including those in the EYFS. Our intention is to fulfil our School's Aims and Objectives.

E-safety is part of the school's duty to safeguard pupils. This policy needs to be read in conjunction with policies regarding; **PSHCE, ICT/Computing**, **behaviour, safeguarding, anti-bullying, data handling, social media, pupil acceptable use, and the correct use of images.** It has been written with close reference to the Teaching Online Safety in Schools government documentation (June 2019).

Using this policy

E-safety is every teacher's responsibility, but the persons designated for overseeing E-Safety at Lanesborough are Nick Williams, Head of Computing, and Alison Heath-Taylor, Head of PSHCE.

Our E-safety Policy pays due regard to government guidance and best practise. It has been approved by senior management and governors.
The E-safety policy is to be revised annually or when changes in legislation are released.
The E-safety policy covers the use of all technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site. This includes, but is not limited to workstations, laptops, mobile phones, tablets and hand-held games consoles used on the school site.
The E-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.
The E-safety policy acknowledges the Home Office/DFE document 'How Social Media is Used to Encourage Travel to Syria and Iraq Briefing Note to School' and is in-line with the 'Prevent' regulations.

Managing access and security

The school provides managed internet access to its staff and pupils. Pupils know how to safely access the web, to aid their knowledge and learning, whilst mindful of the rules to keep them safe on-line. They understand the protocol which bridges the gap between school IT systems and the more open systems outside school

The school uses a recognised internet service provider- at present Virgin Media Business.

The school has an internet filtering system provided by iBoss. This system provides real-time content analysis and is flexible to block different sites for different groups of pupils and adults. We are also able to block any sites which may encourage radicalisation. This will be regularly checked to ensure that it is working, effective and reasonable.

In addition to our internet and network filtering, we run network management software IMPERO. The package was designed in response to UK Government requirements, such as the Prevent duty and the Department for Education's Keeping Children Safe in Education guidance (KCSiE). This monitors device used by pupils at school and laptops which are taken home.

The school ensures that its networks have virus and anti-spam protection. Access to school networks will be controlled by **personal** passwords according to the *Lanesborough Password Policy.*

Use of the internet can be monitored and a log of any incidents kept to help to identify patterns of behaviour and to inform E-safety policy.

The security of school IT systems are reviewed regularly.

All staff that manage filtering systems or monitor IT use are supervised by senior management

The school ensures that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

The school provides an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families takes place using school equipment and/or school accounts according to the Lanesborough Staff Personal Device Usage and Data Handling policy.

Pupils are advised not to give out personal details or information which may identify them or their location

Learning to evaluate internet content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum and through our PSHCE curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. "fake news");
- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

The school actively takes part in, and promotes, 'Safer internet day', each year.

E-mail
Full email use and compliance guidance can be found in our Lanesborough Email Code of Practice policy document. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Boys from Years 5 are given email accounts run using the Google Apps for Education framework. Boys are taught how to use the email system sensibly, safely and shown what to do if they become aware/suspicious of any behaviour which contravenes the Lanesborough Pupil Acceptable Use Policy.

All accounts are accessible to the technical team, with admin privileges and authority to investigate issues and report their findings to the senior management team.

Use of Mobile Phones and Cameras Mobile Telephones:

- Staff may only access their mobile phones during working hours, when pupils are not present and staff are not engaged in the process of teaching.
- The Head of RGS and the Head of Lanesborough can give permission for staff to access their mobile phones during teaching time, if family emergencies so dictate.
- Staff working within the EYFS must store their mobile phones out of the classroom areas during working hours.

Cameras:
Photographs taken for the purpose of recording a pupil or group of pupils participating in activities or celebrating their achievements is an effective form of recording their progress. However, it is essential that photographs are taken and stored appropriately in order to safeguard the pupils in our care.

- Cameras on mobile phones may not be used.
- Only designated school cameras may be used to take images of pupils within the School setting or on outings. Sometimes outside providers may be appointed by the School to take photographs of pupils for media purposes, for the website, for marketing or for personal use. All parents must sign consent for this. The Head of RGS and the Head of Lanesborough are responsible for checking the list of pupils where consent is withheld. They need to ensure that images of these pupils do not appear on the School's website or in the media. Images taken on these cameras must be deemed suitable without putting the pupil/pupils in any compromising positions that could cause embarrassment or distress.
- Images taken and stored on the camera must be downloaded by designated staff as soon as possible.
- Photographs may be distributed to other members of the staff in order to update pupil achievements, or for recording purposes.
- Cameras may only be taken into a bathroom if photographic evidence of children washing their hands needs to be recorded, as is sometimes required by EYFS. This activity must be properly supervised by appropriate staff.

Published content e.g. school web site, school social media accounts

The contact details are the school address, email and telephone number. Staff or pupils' personal information will not be published. No identifiable information will be used online on public facing pages.

The website manager has overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

The vast majority of people who take or view photographs or videos of children do so for entirely innocent and acceptable reasons. Sadly, some people abuse children through taking or using images, so staff have the following safeguards in place.

To protect pupils, as a school:

- Written permission is obtained from parents or carers before photographs of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of pupils.
- Surnames of children are not used alongside any images of pupils.
- Ensure pupils are appropriately dressed
- Ensure that no personal data is shared being GDPR compliant
- Store all images securely on our secure GDPR compliant Sharepoint system.
- Use only school equipment. I.e. not personal devices (See ICT – RGS Staff Data Handling & Device Use Policy
- Encourage pupils to tell staff if they are worried about any photographs that are taken of them.

Use of social media

The school has a separate social media policy**.** The school controls access to social networking sites and considers how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating pupils in their use.

Staff and pupils should use ensure that their online activity, both in school and out, considers the feelings of others and is appropriate for their situation as a member of the school community. Pupils and parents sign the *Lanesborough Acceptable Use Policy* annually.

Use of personal devices

Personal equipment may be used by staff to access the school IT systems provided their use complies with the e-safety policy, staff code of conduct and the relevant AUP.

Use of personal devices is clarified in the *Lanesborough Staff Personal Device Usage and Data Handling policy,* Staff Handbook and Code of Conduct. The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Policy Decisions

Authorising access

All staff (including teaching assistants, support staff, office staff, pupils, teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.

The school maintains a current record of all staff and pupils who are granted access to school IT systems.

In EYFS and Key Stage 1, access to the internet is by adult demonstration with supervised access to specific, approved on-line materials.

At Key Stage 2, access to the internet is with teacher permission with increasing levels of autonomy.

Persons not employed by the school must read the Guest AUP before being given access to the internet via school equipment.

Parents are asked to sign and return a consent form to allow use of technology by their pupil in the form of the *Lanesborough Acceptable Use Policy.*

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints
Complaints of internet misuse will be dealt with, according to the school behaviour policy.

Complaints of a child protection or safeguarding nature will be dealt with in accordance with school's safeguarding procedures.

Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the school's Behaviour Policy. See the *Lanesborough Behaviour and Sanctions policy*.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously. The anonymity that can come with using the internet can sometimes make people safe to say and do things that they would otherwise would not do in person. It is made clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

Any incidents of cyberbullying will be dealt with in accordance with the school's Behaviour Policy, Anti-Bullying Policy, Rewards and Sanctions policy and where appropriate, the school's Safeguarding and Child Protection policies and procedures.

Community use of the internet

Members of the community and other organisations using the school internet connection will have read the guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

To pupils

Pupils need to agree to comply with the Lanesborough AUP to gain access to the school IT systems and to the internet. This is done at the beginning of each school year.

Pupils will be reminded about the contents of the AUP as part of their E-safety learning.

To staff
All staff know where to access the E-safety policy and why it is important.

All staff must sign and agree to comply with the Lanesborough Staff AUP to gain access to the school IT systems and to the internet.
All staff receive E-safety training on a bi-annual basis

To parents
The school asks all new parents to sign the parent/pupil agreement when they register their child with the school.

Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters and on the school web site.

Parents will be offered e-safety training bi-annually.

Signed:

Reviewed Trinity Term 2019

To be reviewed Trinity Term 2020

Appendices
Lanesborough Password Policy
Lanesborough Email Code of Practice 2018-219
Lanesborough Acceptable Use Policy 2018 – 2019
Lanesborough Social Media Policy 2018 – 2019
Lanesborough Staff Acceptable Use Policy 2018 – 2019
Teaching Online Safety in Schools June 2019
ICT – RGS Staff Data Handling & Device Use Policy