Grovelands
Primary School

Grovelands Online Safety Policy

Date of approval:	**Autumn 2018**
Next review date:	**Autumn 2019**
Responsible staff member:	**Mr Daniel Tuck**
Policy reviewed by:	**Craig Smith/ Daniel Tuck**
Sources used for review:	**Guidance from The Key on DfE changes**
Committee/GB responsible:	**Teaching and Learning Committee**
Signed by the Chair of the Governing Body:	**Mr Dean Furber**

ONLINE SAFETY POLICY

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Google Hub and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Radio Broadcasting
- Music Downloading
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Grovelands School, we understand the responsibility to educate our pupils on eSafety 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, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities.

Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Policies are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, PDAs and portable media players, etc).

At Grovelands School, Daniel Tuck is the named lead for Online Safety.

Managing Internet Access

School ICT systems security will be reviewed regularly by the School Business Manager. Virus protection will be updated regularly and security strategies will be discussed with the Local Authority.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable (LGFL/ Securly).
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy (Securly).
- The security of school IT systems will be reviewed regularly.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered.

Internet Use

The school will provide an age-appropriate Online 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 will take place using school accounts.

Pupils will be advised not to give out personal details or information which may identify them or their location. This includes during the use of applications, games, social media sites and programs both inside and out of school in line with our Safeguarding and Child Protection Policy.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.

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

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Head of School or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

Written permission will be obtained from parents or carers before photographs or names 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 children.

Use of social media

- The school has a separate social media policy.
- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Staff and pupils should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the Online Safety policy and the relevant Acceptable Use Policy.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising Access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff Acceptable Use Policy' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the school must read and sign a Guest Acceptable Use Policy prior to being given access to the internet via school equipment.
- Parents will be asked to sign and return an acceptable use policy to allow use of technology by their pupil.

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. Neither the school nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

Teaching e-Safety

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety.

The school has a framework for teaching internet skills in ICT/ PSHE lessons.
The school provides opportunities within a range of curriculum areas to teach about E-safety.
Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum.
Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the

internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Internet Access
The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head of School, School Business Manager or Computing coordinator.
- It is at the Head of School's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.
- All staff have the right to request that a website be unblocked by the Network Manager for pupil use. It is the responsibility of the person requesting the website unblock to thoroughly check the website for inappropriate content.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator.
- The child protection team will regularly check reports on inappropriate use of school computers.

Communication of the Policy
To pupils

- Pupils need to agree and sign to comply with the pupil Acceptable Use Policy in order to gain access to the school IT systems and to the internet
- Pupils will be reminded about the contents of the Acceptable Use Policy as part of their Online Safety education

To staff

- All staff will be shown where to access the Online Safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff Acceptable Use Policy in order to gain access to the school IT systems and to the internet
- All staff will receive e-safety training on an annual basis

To parents

- The school will ask all new parents to sign the Acceptable Use Policy when they register their child with the school.

- Parents’ and carers’ attention will be drawn to the School Online Safety Policy in newsletters and on the school web site.
- Parents will be offered Online Safety training through a bi-annual Parent Workshop.

Links to Other Policies and documents

This policy should be read in conjunction with the;
Acceptable Use Policy
Computing policy.
Safeguarding and Child Protection Policy
Behaviour Policy