# Ripley Court School

## 5 School Rules including guidance policy on the use of ICT, Social Media, Mobile Phones, WiFi and other electronic devices

This policy applies to the whole school, including EYFS. It should be read in conjunction with policy 5a, Acceptable Use

**School Rules**

It has long been the policy of this school not to attempt to create an exhaustive list of school rules, as this is invariably a self-defeating task. The following guidance is issued, however:

1. The staff and parents of the school are expected as a matter of course in all dealings to be proactive in promoting and encouraging excellence in behaviour.
2. The school, however, reserves the right to judge the pupils behaviour by the normal criteria of only accepting the highest standards and to take whatever action is necessary to protect its community and itself.
3. Respect is the key word in behaviour. All members of our community should conduct themselves by respecting themselves and other people, their possessions, their rights and their dignity.
4. Good manners are to be encouraged at all times.
5. The misuse of any technology or bringing the school’s name or reputation into disrepute is a serious offence and may result in exclusion.
6. Dangerous horseplay, fighting or play-fighting is not allowed and offenders may receive sanctions including exclusion.
7. There are areas of the school where children may not go. These include all areas which may not be safe without supervision but specifically:
    a. The workmen’s shed and the fenced-off areas and the bin area next to the school front gates.
    b. Do-little.
    c. The kitchen.
    d. The pond area without supervision.
    e. The theatre lighting box without supervision.
    f. The back car park without supervision.
    g. The walled garden or headmaster’s garden without supervision.
    h. Any locked room or cupboard.
8. The conditions of the school/parent contract take precedence.

**Computers in the curriculum**

Technology has transformed the entire process of teaching and learning at Ripley Court school. It is a crucial component of every academic subject, and is also taught as a subject in its own right. Nearly all of our teaching areas are equipped with electronic whiteboards, projectors and computers. We have an ICT suite in the school and pupils may use the machines there and elsewhere for private study if supervised. We also have mobile internet-connected devices for use in the classroom.

All computers are connected to the internet, which is available to valid users of the system, but unsupervised internet access, despite our filtering system, is not allowed. All of our pupils are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution. However, all users should be aware that sites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, jihadist or other propaganda. Some free, on-line encyclopaedias do not evaluate or screen the material posted on them.

**The role of technology in our pupils' lives**

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, or PSPs (play stations portable), like Wiis and Nintendo DS, together with Bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging) services (like Twitter), to skype (video calls, via web cameras built into computers, phones and PSPs), to wikis (collaborative web pages), chat rooms social networking sites (such as Bebo, Facebook, MySpace, Snapchat and Instagram) and video sharing sites (such as YouTube).

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of our role at Ripley Court to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all of our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for our Computer department, our Child Protection Officer and our pastoral staff.

Our technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of computers. They monitor the use of the internet and emails and will report inappropriate usage to the pastoral staff.

**Role of our Designated Safeguarding Leads (DSL)**

We recognise that internet safety is a child protection and general safeguarding issue.

Our Child Protection DSLs have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. They work closely with the Surrey Safeguarding Children's Board (SSCB) and other agencies in promoting a culture of responsible use of technology consistent with the ethos of our school. All of the staff have also received training in e-safety issues. The school has a comprehensive Personal Social Health and Economic Education programme and this together with training by the Head of Computer Science aims to ensure that all year groups in the school are educated in the risks and the reasons why they need to behave responsibly online.

**Misuse: Statement of Policy**

We will not tolerate any illegal material, and will always report illegal activity to the police and/or the SSCB.

If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP).

We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy. This may include exclusion.

**Involvement with Parents and Guardians**

We seek to work closely with parents and guardians in promoting a culture of e-safety. We will always contact you if we have any worries about your son or daughter's behaviour in this area, and we hope that you will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. We therefore arrange regular discussion and training evenings for parents when an outside specialist advises about the potential hazards of this exploding technology, and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity.

## CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT RIPLEY COURT

E-safety is a whole school responsibility, and at Ripley Court, the staff and pupils have adopted the following charter for the safe use of the internet inside the school:

### Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be so pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. Our school's anti-bullying policy describes our preventative measures and the procedures that will be followed when we discover cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe computing environment at school; but everyone needs to learn how to stay safe outside the school.
- We value all of our pupils equally. It is part of our ethos to promote considerate behaviour, and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff and dealt with under the auspices of our anti-bullying policy.

### Treating Other Users with Respect

- We expect pupils to treat staff and each other online with the same standards of respect as they would in the course of face to face contact.
- We expect a degree of formality in communications between staff and pupils, and would not normally expect them to communicate with each other by text or mobile phones, unless specified under other policies such as on educational visits.
- Lists of mobile phone numbers and contacts should not be kept after any such trip.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. Ripley Court is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other, and to report any concerns about the misuse of technology, or worrying issue to a member of the pastoral staff.
- The use of cameras on mobile phones is not allowed.

### Keeping the School Network Safe

- Certain sites are blocked by our filtering system and our computer department monitors pupils' use of the network and email traffic.
- We do not issue pupils with their own personal school email address.
- Access to the school system is via secure personal LOGON, which is password protected. We give guidance on the reasons for always logging off and for keeping all passwords securely.
- We have strong anti-virus protection on our network.
- Any member of staff or pupil or guest, who wishes to connect a removable device to the school's network, will have to obtain a password from the headmaster or bursar. The use of the network constitutes an agreement to abide by this policy.

**Promoting Safe Use of Technology**

Children are taught about the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. Guidance covers topics such as saving yourself from future embarrassment and protection of your "NetRep", explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

**Safe Use of Personal Electronic Equipment**

- Our guidance is that no one should put anything onto the web that they would not say to their grandmother!
- We recommend strongly that parents do not allow children onto social networking sites until they ore of a suitable age (usually 13 14) We teach about cyberbullying in PSHE and computer lessons.
- Our PSHE lessons include guidance on how pupils can identify the signs of a Cyber-stalker, and what they should do if they are worried about being harassed or stalked online.
- We offer guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- We give guidance on how to keep safe at home, by encrypting your home wireless network, not opening unknown attachments and reporting any illegal content. Similarly we cover how a mobile phone filter can be activated, and how to block nuisance callers.

**Considerate Use of Electronic Equipment - children**

- Mobile phones are not banned but are not encouraged at school. The school takes no responsibility for toys or other electronic devices. If at school, they should be switched off, or taken to reception for storage.
- iPods and other personal electronic devices are banned from the school site.
- Staff may confiscate personal equipment if found, or mobile phones if a nuisance.
- Sanctions may be imposed on pupils who use their electronic equipment without consideration for others.

We expect all pupils to adhere to these requirements for the safe use of the internet. Copies of this are available on the school's website. At age 11 (year 6), all children and their parents are asked to sign an Acceptable Use Policy.

**Note for teachers and other adults**

- Staff and adults are to be very careful in the use of cameras, in particular those on Mobile Phones, which may enable pictures to be sent more easily electronically. It is not expected that staff taking pictures of children for profiles or records of any sort will use personal mobile phones to do this. In particular, mobile phones should not be used in the EYFS settings at all.
- Teachers have a contractual requirement to observe the requirements of the Data Protection Act and to keep data safe. This means that the storage off site (which is not recommended) or transmission of data of sensitive information should at least be encrypted, and any PC, tablet or storage medium be held secure.
- Teachers must be careful in their use of social networking sites, such as Facebook, Twitter or similar. This included who they are "friends" with, who they follow, and what they themselves post on the internet. They should at all times consider that the contents of any online postings, email and other electronic attachments could easily become public and they may well be held responsible for their opinions, even in the

context of the wrong audience.

- In particular they should not to be “friends” or contacts with any parent or pupil on any social media sites, and must not communicate with parents, staff or pupils using these networking sites.
- The school will not accept responsibility for losses to any staff using the school’s network or equipment to conduct business, internet banking or any other personal business. The schools equipment is to be considered a “Public Network” and protection on this network from internet fraud, damage to personal equipment or similar may not be presumed.

Background and references for further information from the ISBA:

A Legal Requirement, & an ISI Reporting Standard,
An OFSTED Reporting Standard for Boarding Schools

References:
ISI Handbook 2015
https://www.getsafeonline.org/
Childnet International
UK Safer Internet Centre - a partner of Childnet International, South West Grid for Learning and the Internet Watch Foundation: co-funded by the European Commission's "Safer Internet Programme"
The South West Grid for Learning - one of the three charity partners of the UK Safer Internet Centre
Child Exploitation and Online Protection Centre - a National Crime Agency command dealing with criminal / safeguarding concerns and reporting