



# LOCHINVER HOUSE

## Acceptable User and Cyber-Security Policy – Pupils

---

### Purpose

- To safeguard and protect the pupils and staff of the School
- To allow all users to access and use the Internet safely at School
- To protect all users from sites, information and individuals which could cause distress to users and undermine the aims and principles of the School
- To provide clear rules which are consistent with the School rules

### Expected Conduct

#### The Pupils:

- Are responsible for their individual account and must take all reasonable precautions to prevent others from being able to use it
- Must not share passwords or logon details with anyone other than IT support within the School
- Will promptly disclose to a member of staff any inappropriate messages, or any online content which makes them feel uncomfortable
- Will promptly report any knowledge they have about another pupil who is the victim of cyber-bullying
- Must not open any emails or attachments received from an unknown sender. These should be reported to a member of staff or IT immediately
- Must not connect to a computer any device that has not been provided by the School (such as a USB memory stick) without first seeking permission from a member of staff
- Are responsible for communicating politely in online environments both inside and outside of the School
- Must recognise that taking the ideas, text or pictures of others and claiming they are your own is intellectual theft (plagiarism)
- Will not take or distribute photographs or videos of staff or pupils without their knowledge and permission
- Should assume that messages and content posted online cannot be deleted and must therefore use the 'stop and think' approach before doing so
- Should seek advice from an appropriate member of staff if they are unsure whether a particular action is acceptable

### No activity should be undertaken which shows disrespect for the School or the School community

### Incident Management

- Incidents of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy
- Incidents of inappropriate language and/or Internet use by pupils are captured by Securus and reviewed by the Online Safety Officer. This information may also be passed to the Deputy Headmaster
- Sanctions are awarded for any inappropriate use of IT systems in line with the School's Behaviour Management, Reward and Sanctions and Exclusions Policy



Any pupil who knowingly commits an offence will be accountable for their actions in line with the School's Behaviour Management, Reward and Sanctions and Exclusions Policy. Offences include, but are not limited to:

- Cyber-bullying
- Hacking
- Intellectual theft
- Accessing or sending inappropriate material or messages
- Sending emails to large groups of users (spamming)
- Accessing the account or files of others
- Purposefully bypassing controls and limitations placed on School systems and devices
- Causing wilful damage to school IT facilities
- Introducing viruses to the network

---

Policy Reviewed: 20.07.2018  
Policy Review Date: 19.07.2020  
Policy linked to: Anti-Bullying Policy, Behaviour Management, Reward and Sanctions and Exclusions Policy, Data Protection Policy, Mobile Telephone Policy - Pupils, Privacy Notice, Pupil-Parent iPad Agreement

*Any data held in relation to the content of this policy will be managed in accordance with our Data Protection Policy and Privacy Notice.*

