FINTON HOUSE
SCHOOL

ACCEPTABLE USE POLICY (FOR PARENTS)

Member(s) of staff responsible: Ben Freeman

Date Revised: 10 April 2018

Governing committee/sub-committee responsible: Safeguarding

A copy of this policy is available to all governors and parents via the school website or a hardcopy on request from the School Office. It is accessible to all staff electronically (in the Policy folder on the Staff Admin Drive) and a hardcopy held on file in the Head's Office.

Contents

1. Policy Statement

Finton House Schools' Acceptable Use Policy aims to create a safe digital environment for all aspects of technology used throughout the school. The purpose of this policy is to ensure that children and parents are educated about the benefits, risks and responsibilities of using information technology. All staff, pupils, and parents are expected to play a part in ensuring this policy works well in practice. This policy applies in addition to the School's other relevant terms and conditions and policies, including

The School's terms and conditions (parent contract)

- the School's Data Protection Policy
- the School's Technology Policy
- the School's Images Of Pupils Policy
- the School's Retention of Records Policy
- the School's Safeguarding Policy

2. Mobile Technologies

Mobile technology devices may be school owned or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network.

School Devices

School owned mobile devices (laptops, iPads, cameras etc) are used for educational purposes. They can be booked out by staff for children to use. The School manages all of these devices, including the monitoring of their use.

Appropriate access is applied to all devices according to the requirements of the user, and filters are applied to the internet comnnection which no one is permitted to bypass. Proactive monitoring has been implemented to monitor all online activity.

Personal Devices

Children are allowed to bring personal devices into school with permission from a teacher, and to support their learning. They may only be used in lessons in accordance with teacher direction. Year 6 pupils may bring in a mobile phone if they are walking home alone, but phones must be handed into the office on arrival at school.

Personal devices belonging to parents such as mobile phones, cameras, home laptops, iPads or any mobile technology are brought into school entirely at the user's own risk and the school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school. Neither does the school accept any responsibility for any malfunction of a device while on the school network or whilst resolving any connectivitiy issues.

Devices must be set to silent mode when on the school site.

Personal devices should be made easily identifiable and in a protective case to secure them. Passcodes or PINs should be set to aid security.

All personal devices are restricted to provide appropriate levels of network access.

The school reserves the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.

Technical support is not available in school for personal devices. Users are responsible for keeping their device up to date through software, security and app updates.

Devices must be virus protected and not be capable of passing infections to the network.

3. Use of Digital and Video Images

Staff and parents are encouraged to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images.

Parents are required to give consent to their children's images being used at school. This consent is given via the Parental Consent (Images) Form.

Parents are welcome to take videos and digital images of their own children at school events for their own personal use (as such use is not covered by the Data Protection Act). To protect everyone's privacy and in some cases protection, these images should not be published by parents or made publicly available on social networking sites, nor should parents comment on any activities involving other children in the digital / video images.

Children must not take, use, share, publish or distribute images of others without their permission.

Care should be taken when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Children's full names must not be used anywhere in the public domain, particularly in association with photographs. Children's work can only be published with the permission of the child and parents or carers. Staff are aware of the school list of any children for whom such permission has not been given.

4. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

It is the responsibility of all members of the school community to take care when handling using or transferring personal data so that it cannot be accessed by anyone who does not:

- Have permission to access that data;
- Need to have access to that data.

Any data that can identify an individual must be handled safely and securely by everyone in the school to minimise the risk of its loss or misuse.

Parents are given access to a range of personal information about members of the school community including names, addresses, contact details, class lists, children's work and family information. This information must only be used for the purpose it is intended, and must be securely destroyed when finished with.

Personal data must never be shared with a third party outside the school community (eg. friends, neighbours, family members or business associates) without the permission of the subject.

Parents or pupils transporting personal data on a portable device or other removable media (camera, smartphone, laptop) must ensure the data is encrypted and password protected. The data must be securely deleted from the device once it has been transferred or its use is complete. For further information about handling personal data please refer to the schools' Data Protection Policy.

5. Digital Communications

All staff and Upper School pupils are provided with a school email account which is secure and monitored. Staff and pupils should only use their school email accounts to communicate with others when in school or on school systems.

Children are not permitted to use personal devices, personal email addresses, private messaging apps, social media, or blogs in school or on the school network.

Parents are encouraged to communicate with staff via the school email network. Any digital communication conducted between parents and staff (email, social media, chat, blogs, VLE etc) should be polite and professional in tone and content, and take place on official, monitored school systems. Staff are required to access their emails on a regular basis to ensure mail is responded to in a timely manner, however staff cannot access emails during lessons, duties or clubs, so it may take up to one working day for them to reply. Parents should not contact staff via their personal mobiles or personal email accounts.

Improper or inappropriate personal use of the School's Internet and email systems may result in disciplinary action. We expect that any pupil using the School's email system will exercise their right to freedom of expression with due consideration for the rights of others and in accordance with the AUP Terms of Use.

Any user must report to the Head or a senior member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

6. Use of Social Media

Pupils

It is not expected that any Finton House pupil will have access to social media without parental supervision, because thirteen is the minimum age for account holders on all the major social media sites.

Guidance for Pupils

- The School's advice is that no pupil at Finton House should be accessing social media applications.
- No pupil should attempt to access social media via another person's account. If such an attempt is made, the Head and the child's parents should be informed.
- Any attempts to breach the school's filtering system Smoothwall will result in disciplinary action.
- Any pupil messaging a school group (e.g. their class) via social media or any digital means on a personal device or personal account is considered to be subject to the terms of the school's AUP. Any such activity is goverened by the same rules, guidelines and disciplinary procedures as it would be if it took place in school on a school device.
- Any improper contact or bullying should be reported immediately to the class teacher or any senior member of staff.
- The School has a zero tolerance to bullying whether online, offline, at home or at school.

Parents

The School expects that any parent interacting with the school via a school social media account will exercise their right to freedom of expression with due consideration for the rights of others and in accordance with the AUP terms of Use.

Social Media:

- should not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school or a member of the school community into disrepute.
- should not be used in an abusive or hateful manner
- should not breach the school's safeguarding, equal opportunities or bullying policies
- should not be used to discuss or advise any matters relating to school staff, pupils or parents
- Users should make it clear that any personal opinions are their own and are not attributed to the school.

7. Moderated mailing lists, newsgroups and chat rooms

Pupils

- Teachers will moderate other collaboration tools such as newsgroups and chat rooms if used on the school network for learning purposes.
- Pupils will be denied access to public or un-moderated chat rooms.
- Only regulated educational chat environments shall be used. They will always be used under supervision. Safety is the major consideration.
- Only newsgroups that have educational goals and content will be made available to pupils.

8. Unsuitable / Inappropriate/Illegal Use

Pupils

Section 19 of the Technology and Online Safety Policy deals with potential incidents of mis-use by pupils. These include unauthorised or inappropriate use of devices, apps or websites, attempting to access sites, accounts or data from which they are banned, sending messages texts or emails that are offensive, harassing or bullying in nature, or infringing copyright. Pupils will be made aware that infringements of the school's policy will have serious consequences and could lead to the involvement of the Police.

Parents

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying is also banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context e.g. promotion of any kind of discrimination or extremism, using school systems to run a private business or infringing copyright.

Parents may refer to Sections 17 – 19 of the Technology and Online Safety Policy for further information regarding: Unsuitable or Inappropriate Activities, Incidents of Mis-use, and School Actions and Sanctions.

9. Technical security, Filtering and Passwords

The School's computer network security systems and virus protection software are reviewed and updated regularly by Finton House School's computer service provider. Pupils must take care not to try and bypass this protection, and make sure that any device they bring into school is similarly protected in order not to transmit infections to the school network.

The "Smoothwall" filtering system monitors and records user activity and is fully compliant with "Keeping Children Safe in Education". The Head, DSL and safeguarding governor regularly "dip test" (monitor and record) the activity of all users on the school technical systems. Records of all activity are kept for 2-3 months. The content of internet sites being accessed by users via the school internet connection is continually filtered, whether on a personal or school owned device.

The School allows pupils clearly defined access to school technical systems. These are accessed via a personal login and password which must be kept secure and not shared with anyone. Lower School pupils will use class log-on or common passwords. Upper School pupils will have a unique password of at least 6 letters/ numbers.

10. Education and Awareness

Informing parents and children

"Smart Rules" posters will be displayed in the computer room. The computing curriculum includes units of work for all year groups on safe and responsible use of the Internet. Parents' attention is drawn to the relevant school policies on the website. Parents will also be kept up to date with advice relating to safe internet use at home via newsletters and workshops.

Informing parents and Pupils about the school's AUP

All parents will be provided with a copy of the School's AUP. Parents and pupils are aware that Internet traffic can be monitored and traced to an individual user.

Parents will be asked to sign a statement to say that they have read and understood the AUP and agree to abide by its terms, and that they have explained the terms of the AUP to their children. Parents should be aware that they are signing on behalf of their children who are pupils at the school. However, Upper School pupils will go through a simplified version of the AUP at school and sign a copy to say that they have understood it and agree to abide by its terms.

11. Terms of Use for Parents

The School Network

- I will teach my child the importance of keeping passwords secure. I will encourage my child to log out after each session and never allow other users to use his/her username and password. I will report any suspicion, or evidence that there has been a breach of my child's personal security to the Headmaster.
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the school's computer service provider.
- I understand that the use of the network or school devices without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- I understand that my child's files, communications and internet activity is monitored and checked at all times to protect his/her own and others' safety, and action may be taken if deemed necessary to safeguard him/her or others.

Social Media

- I will monitor my child's use of the internet, especially social media sites, and take all reasonable steps as a parent to promote and safeguard my child's online safety.
- When using school accounts, content should be polite and respectful at all times. I will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgements about other members of the school community.
- When using a personal social media account, I must make it clear that I am not representing the School.
- I will not use a personal social media account to to discuss school matters, staff, pupils or parents.
- I must not publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. I am aware that if my out-of-work activity causes potential embarrassment to the School or detrimentally affects the School's reputation then the School is entitled to take disciplinary action.
- I understand that I must not put children at risk by identifying them online.
- I may not use the school's internet, email or network system for the promotion of personal financial interests, commercial ventures or personal campaigns other than with permission from the Headmaster.

Managing Digital Content

- I agree to follow school policies concerning the sharing, distribution and publication of digital images and video that include other people's children.
- I will not allow any digital images or videos that I create of children to be published or made publicly available on social networking sites
- I will not comment on any activities involving other children in digital / video images.
- I will not allow my child to take, use, share, publish or distribute images of others without their permission.
- I will take care when taking digital / video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- I understand that children's full names must not be used anywhere in the public domain, particularly in association with photographs.

Parents will be sent a copy of this School's Acceptable Use Policy (AUP). They will be asked to confirm that they have read and understood this policy and agree on behalf of themselves and of their child to abide by its terms.

Upper School pupils will go through a simplified version of the AUP at school and sign a copy to say that they have understood it and agree to abide by its terms.