ABINGDON

ICT & E-Safety Policy (Pupils)

Digital and Electronic Resources At Abingdon School

This policy must be read in conjunction with all other Abingdon policies, paying particular to regard to the Data Protection Policy, the Safeguarding Policy and the Anti-Bullying Policy.

Who Needs To Operate Under This Policy?
This policy applies to pupils at Abingdon Senior School. Please see separate policy for Abingdon Prep School.

The Range of Resources Covered

- School data and information held in a digital/electronic environment.
- School infrastructure providing, enabling and managing digital and electronic resources.
- Digital (including computer) and electronic hardware and software.
- Photocopiers, scanners, printers and audio visual e.g. projectors.

1. Background and Purpose

1.1 Pupils need to use digital and electronic resources as part of their education at Abingdon School. These resources, owing to their nature, may be subject to rapid change and development.

1.2 Pupils are required to be aware of and adhere to the laws of this country and to follow the policies of the school and the instructions of staff. School instructions and guidance relating to behaviour, bullying, use of the internet and social media as well as guidance in use of mobile devices (including phones) need to be considered with this policy along with other relevant aspects of academic and PHSCE teaching. If a pupil is unsure about this they must speak to their teacher, tutor or housemaster. If a pupil observes activity in breach of this policy they must inform a member of the academic staff. For the reporting of this, or of any other inappropriate behaviour, it is also possible to use the school's whistleblower email address, whistleblower@abingdon.org.uk, also available via the whistleblower link on all Abingdon Firefly dashboards.

1.3 The School is required to manage and use all data and information as described by the Data Protection Act 1998, the School's Data Protection Policy(ies) and Privacy Notice . The Director of Finance and Operations is the Data Controller for the School. Any queries relating to the management and use of data and information should be directed to an academic member of staff e.g. subject teacher, tutor, or housemaster, in the first instance. If need be, then contact The Director of Finance and Operations.

1.4 Within the context of 1.1 to 1.3 above this policy aims to provide a framework for and an explanation of the pupil acceptable use of digital and electronic resources at Abingdon School. The range of resources available is extensive and is not limited only to the use of, for example, the school network, computer hardware and software, the internet and the world wide web. This policy intends to give direction to pupils on the acceptable use of digital and electronic resources. Any queries need to be directed to the Deputy Head Pastoral or the ICT Manager.

2. Data Supply, Quality and Integrity, including infrastructure and connectivity.

2.1 The School provides digital and electronic resources of appropriate quality which include an internet supply which is appropriately monitored and filtered for use by the School community in the delivery of their day-to-day school business. At times this provision, due to circumstances inside or outside of the control of the School, may be unavailable. The School will work appropriately to restore the required service. At such times the School asks pupils to use, where possible, non-digital methods of working to the best of their ability.

2.2 Pupils should not knowingly take action that will damage and/or compromise the speed, quality, integrity of the data and/or infrastructure and services supplying data, information and other digital and electronic resources to the School community.

2.3 Pupils should not connect to the School network other than in the way(s) directed by the IT Manager and his/her team. Personal devices should always connect to the school network over WiFi - never connect personal devices by network cable.

2.4 Pupils have personal login details to enable them to use the School's IT resources. Pupils have personal login details to enable them to access selected information and online IT resources. A pupil should never use another person's login details, nor should they, under any circumstances, share any of their personal login details with any other person, including teachers or other pupils. If a pupil thinks that their login details might be compromised they should immediately contact the ICT team by telephone (x266) or by email (support@abingdon.org.uk) and request that their login password(s) are reset.

2.5 Passwords should be reset regularly and should be chosen to be as secure as possible. A pupil can get further advice on this by emailing support@abingdon.org.uk.

2.6.The digital and electronic resources that can be removed from the school must not be removed from the school without permission of a member of staff.

2.7 It is expected pupils will respect the need for the avoidance of waste and the importance of using equipment sustainably. This particularly refers to the use of printers and copiers within the Abingdon Foundation.

3. **Management and Storage of Data**

3.1 Pupils should save work in Google Drive. Work saved locally on school computers will NOT be saved permanently or backed up.

3.2 Images and video should only be taken as part of the pupil's education and boarding day-to-day school life with the knowledge and permission of a member of staff.

Deputy Head Pastoral
IT Manager
Last internal review: September 2018
Last governor review: May 2018
Next governor review: May 2019

Appendices.

The following documents are provided in the Appendices, are on Firefly, and are explained to pupils by Tutors and Housemasters:

1. Practical advice on ICT Acceptable Use (including how the School monitors the network)
2. Cyberbullying
3. Advice for Children
4. Student Device Guidelines Poster

Appendix 1

Some Practical Advice on ICT acceptable use

The overall aim for Information and Communication Technology across the Abingdon Foundation is to enrich learning for all pupils, to support their academic studies, online safety, pastoral care and recreational interests and to promote effective communication.

Duty of care

Abingdon has a duty of care towards every member of the Foundation to ensure the safe use of computing facilities. By using a school computer or by accessing any of the school's ICT services you agree to abide by the standards expected by the Abingdon Foundation.

Security & Access

The owners of documents and online digital resources are responsible for ensuring that access to those resources is appropriately limited or restricted. The IT department can assist or advise on how to do this if necessary.

Use of the school ICT equipment

Never:

- give your login details to any other person and take all reasonable steps to ensure that they remain known only to you
- attempt to log into a resource using anyone else's login
- become involved in any inappropriate, antisocial or illegal behaviour online
- send offensive or harassing material to others or take part in any form of cyberbullying.
- move, unplug, tamper with or vandalise school computer equipment
- connect any equipment of any description to the school network without written permission from the IT department
- attempt to access inappropriate websites or material by trying to circumvent the school internet filtering system
- create, share, download, display or store files or material that contain unsuitable or offensive language or images
- download, install or attempt to use or run any software on school computers without written permission from the IT department
- undertake or pursue any activity that might threatens the integrity of the school computer network, school online resources or any other network or online systems, or that hacks, attacks or corrupts the network, is forbidden.

Always:

- **n**otify a member of staff if you witness illegal, suspicious or unacceptable behaviour

- notify the IT department (x266, support@abingdon.org.uk) if you have any issues or problems with computer equipment or if you are unable to access school online resources
- notify the IT department (x266, support@abingdon.org.uk) if you discover unsuitable content on school computers or online

Plagiarism
You should be aware of the regulations and school guidelines about copyright and plagiarism. Any passage of text, copied from a public source such as the internet should be acknowledged, giving the site URL where appropriate, author and date. The school's librarians can offer advice, and there is information on Firefly.

E-mail
- You should check your school email account regularly: at least once per day.
- You should attempt to respond to or acknowledge email messages reasonably quickly.
- You are responsible for the emails you send and for contacts you make.
- Do not to provide your address, telephone number or photograph in an email unless the recipient is known to you personally.
- Never share bank account numbers or credit card details by email
- Attachments to emails should be sent as .zip compressed files or, in the case of documents, .pdf files if you do not wish them to be altered by the recipient.

Never:
- transmit obscene, hateful or threatening communications.
- communicate or publish inaccurate, defamatory or racially offensive materials.
- transmit via e mail any unsolicited advertising, junk mail, spam, chain letters, or any other form of e mail solicitation.
- use the email system to commit crimes or to bully, harass or stalk others.
- use the school email system for personal financial gain, gambling, political purposes or advertising.

Cyberbullying & whistleblowing
Behaviour that is of a bullying nature is never acceptable, even if online. Please see the Safeguarding and Anti-Bullying Policies.

If you wish to report inappropriate behaviour you can speak to any teacher or report it anonymously using the school's whistleblower website. You can also find advice on the CEOPS website.

Social networks, blogs and Twitter
You are liable for your online behaviour in exactly the same way as you are liable for your behaviour offline.

Never:
- post anonymous messages, personal remarks or personal details about anyone else or impersonate someone else.
- use photographs of groups or individuals on a website or blog without their permission.
- post or respond to electronic communications or messages that are impolite, indecent, abusive, discriminatory or racist or in any way intended to cause hurt to another person.
- post personal information about yourself, such as your age, hobbies, phone numbers or your address.
- post anything that could be considered upsetting.
- bring the school name into disrepute.

Never use the internet or e mail to arrange to meet someone you do not know. Not everyone is who they say they are.

Boarders
Abingdon School aims to provide boarders with the same internet freedoms they would enjoy at home, but the school has an additional duty of care towards its boarding community to provide a safe, secure and healthy environment in which to live and work.

This includes a duty of care towards the boys with regard to adequate sleep and development of social skills. Long periods spent online or using computers can be a cause for concern and Housemasters will exercise their duty of care when necessary in this regard.

BYOD

- You may be held responsible, at least in part, for the actions of another person if you permit them to use your laptop
- You are responsible for ensuring that your computer equipment is stored securely when it is not being used
- You are responsible for maintaining your own computer equipment, for ensuring that batteries are charged and for backing it up. Aside from help to connect to school WiFi, no technical support, software or maintenance can be provided by the school's ICT department.
- School reserves the right to carry out physical inspections of equipment at any time, including electrical safety testing, and examination of content and data stored on your equipment and any separate storage devices.

Monitoring and Filtering
The school, through the IT department, has a legal duty to monitor the use of computer equipment, internet access and online communications using email and other services so that they are not used inappropriately, for unlawful purposes or to distribute offensive material and so that the health, safety, discipline and security of students, staff and property is protected and maintained. This information may, if necessary, be used in disciplinary actions.

Content filtering is done in real-time and is based on web page content instead of URLs, allowing sites to be more accurately classified and filtered, and without overblocking. The School inspects all traffic for a range of key themes (including terrorism and radicalisation), including encrypted SSL, and actively blocking adult and illegal material, unmoderated image hosting, peer to peer, malware, gambling, dating and adverts, VPNs and Proxies. Traffic to banking and payment websites is not inspected.

The School recognises that children will have access to the internet on 3G and 4G networks outside the School's monitored systems. When using 3G and 4G networks, the School expects all pupils to abide by the rules contained in this policy. Inappropriate use will result in disciplinary action. Pupil mobile phones within School should be used for 'school business' - accessing Firefly, work resources etc.

Sanctions
Depending on the severity of the offence and at the discretion of the head of IT, Housemaster, Deputy Head Pastoral or Head, one of the following will apply:

1. Temporary ban on internet or network use.
2. Permanent ban on internet use.

3. Permanent network ban.
4. Normal school disciplinary action.
5. Police involvement, where appropriate.

Appendix 2

ABINGDON

Cyber-bullying

The DfE has issued very helpful guidance on cyber bullying. They contained hyper links so the best advice would be to look at these online in order to access the resources available. The links to these documents are:

Cyber bullying: advice for Headteachers and school staff
Advice for parents and carers on cyber-bullying

The advice contained within this guidance is embedded in the school policy above, but of particular note to **staff, parents and pupils** would be the following sections:

- the safety and reporting tools for various social networking sites (p5 of the Advice for headteachers and staff)
- the contact details for mobile phone providers (p6 of the Advice for headteachers and staff)
- the Advice for Children (p3 of the Advice for parents and carers) reprinted below
- the information and links on social networking (p1 and 2 of the Advice for parents and carers)
- the information and links on social networking (p2 of the Advice for parents and carers)

There are also regular evening meetings for parents with the Deputy Head Pastoral and either the Lower Master or Middle Master to address online issues. These are published via the weekly mailing.

In addition parents should refer to the **"Pastoral Advice for Parents," ** issued to all parents via the weekly mailing, which contains information on screen time; safer internet use; pornography; social networking and gaming; phones; sleep patterns and screen usage. This can be resent to any parent: please contact the Deputy Head Pastoral, mark.hindley@abingdon.org.uk.

Appendix 3

ABINGDON

Advice for children

The following are some things that parents may wish to consider teaching their children about using the internet safely:

- Make sure you use the privacy settings.
- Always respect others – be careful what you say online.
- Be careful what pictures or videos you upload. Once a picture is shared online it cannot be taken back.
- Only add people you know and trust to friends/followers lists online. When talking to strangers keep your personal information safe and location hidden.
- Treat your password like your toothbrush – keep it to yourself and change it regularly.
- Block the bully – learn how to block or report someone who is behaving badly.
- Do not retaliate or reply to offending e-mails, text messages or online conversations.
- Save the evidence. Always keep a copy of offending e-mails, text messages or a screen grab of online conversations and pass to a parent, a carer or a teacher.
- Make sure you tell an adult you trust, for example, a parent, a carer, a teacher, on the anti-bullying co-ordinator or call a helpline like Childline on 08001111 in confidence.
- Most social media services and other sites have a button you can click on to report bullying. Doing this can prevent a bully from targeting you and others in the future. Many services take bullying seriously and will either warn the individual or eliminate his or her account.
- While you are on your mobile phone make sure you also pay attention to your surroundings.

Appendix 4 - Student Device Guideline Poster

When using technology at school I will:

This means I will:

- Act in a way that is in accordance with being part of a school community
- Live in the moment and not play games or waste time on my phone
- Not use my phone when I could be talking to other people
- Treat people the same online and off, as I would want to be treated
- Let a member of staff know if I see anything that worries me
- Respect the equipment and services made available
- Explore innovative and creative ways to learn
- Use the tools to help be organised
- Not plagiarise or do anything illegal
- Be aware of the School's ICT Policy for Pupils

ABINGDON