



# CROSFIELDS SCHOOL

## IT ACCEPTABLE USE POLICY FOR PUPILS

**Policy Owner:** Director of Digital Strategy

**Reviewed By:** Head, DSL

**Approved By:** Safeguarding Governor

**Review Date:** 26 November 2023

**Next Review Due:** By September 2024

## Contents

1. Introduction .....	3
2. Policy requirements .....	4
3. Access to the School's Wi-Fi network and resources .....	4
4. Acceptable use of devices.....	4
5. Filtering & Monitoring .....	
6. Google Workspace for Education.....	6
7. Long-term care and support of devices .....	6
8. Damage and loss .....	6
9. Technical support.....	7
10. Insurance .....	8
11. Crofields's technology standards.....	8
12. Security and device management processes .....	8

## 1. Introduction

This policy along with the Schools Online Safety Policy sets out the rules for pupils when using all school devices, systems, shared areas and communication services (online and otherwise) and applies when accessing these from outside school. This Acceptable Use Policy also operates as the schools Bring Your Own Device (BYOD) program in Years 7-11 by outlining Crosfields School's expectations for the school, its pupils, and their parents/guardians in relation to the use of pupil devices within the school.

The term 'device' refers to any mobile electronic technology, including assistive technologies, brought into the school, which is owned by the pupil, and which has the capability of connecting to the school's Wi-Fi network.

We realise some families may already have a suitable device at home or would prefer to look for an alternative. This is fine, but please use the details listed in the 'Crosfields Minimum BYOD Device Requirements' document as a guide to selecting a suitable device.

Crosfields cannot guarantee that devices that do not meet the minimum requirements will be suitable for pupils to successfully engage in their learning.

## **2. Policy requirements**

- 2.1. Pupils can bring authorised devices to the school for the purpose of learning. Please note that the school does not currently allow the use of devices that connect to a 3g, 4g or 5g mobile network to be used as part of the BYOD program; this includes all mobile phone and/or mobile phone peripheral devices such as smartwatches.
  
- 2.2. Pupils in year 7 to 11 must read and accept the 'IT Acceptable Use Policy for Pupils' prior to participation in the BYOD program.

## **3. Access to the School's Wi-Fi network and resources**

- 3.1. Internet access through the school's Wi-Fi network will be provided on school premises at no cost to pupils who are enrolled at Crosfields.
  
- 3.2. Access to school resources such as shared drives, printers and associated costs will be a school-based decision.

## **4. Acceptable use of devices**

- 4.1. The Head will retain the right to determine what is and is not appropriate use of pupil devices at the school within the bounds of the school's policies, GDPR and other legislation.
  
- 4.2. The appropriateness of device use by pupils remains at the discretion of the classroom teacher.
  
- 4.3. The consequences of any breaches of the school's IT Acceptable Use Policy for Pupils will be determined by the Head in accordance with relevant school policies and procedures.
  
- 4.4. Pupils must comply with the school's policies concerning the use of devices at the school.

4.5. Pupils should not attach any school-owned equipment to their devices without the permission of the school.

4.6. Pupils should not connect their devices to the school's internal network via Ethernet connection under any circumstances.

4.7. Pupils must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware or software security mechanisms that have been implemented by the school.

4.8. Pupils understand that bullying and harassment can take place online and therefore should be mindful when sending messages or emails to others.

**Appendix B** covers good email and messaging etiquette.

4.9. Pupils must not relocate or interfere with the configuration of any school owned hardware devices.

4.10. Pupils must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

4.11. There may be times when pupils are required to take photographs or make video or audio recordings during learning activities that are supervised by an appropriate staff member.

4.12. Other than in situations outlined in clause 4.10, pupils must not take photographs or make video or audio recordings of any individual or group without the express written permission of each individual (including parent/guardian consent for minors) being recorded and the permission of an appropriate staff member.

4.13. Pupils must not store on their device any content dealing with illegal activities, material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature. Such content may result in disciplinary and/or legal action.

4.14. Pupils must not use the school's network services to search for, link to, access, store, or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature. Such use may result in disciplinary and/or legal action.

4.15. All communication with other users should be respectful, accurate and use appropriately written expression as would be acceptable in a written school assessment. Pupils should never reveal personal details, including addresses or phone numbers to others.

4.16. Pupils must not attempt to steal any data or software from the school network or another device. Such action may result in disciplinary and/or legal action.

4.17. Where the school has reasonable grounds to suspect that a device contains data which breaches the 'IT Acceptable Use Policy for Pupils', a staff member with delegated authority may confiscate the device for the purpose of confirming the existence of the material. The device will not be returned until the incident has been resolved. Depending on the nature of the material involved, school disciplinary action may be appropriate or further action may be taken including referral to the police.

4.18. Pupils must not access software applications or material from their device which are not relevant to their current learning.

4.19. Information published on the Internet may be inaccurate or may misrepresent a person or situation, therefore care must be taken in the use of this information.

4.20. Pupils using their device inappropriately may be asked to close their device and complete their learning activities by alternative means.

4.21. A more pupil friendly version of acceptable use guidelines is available at **Appendix A** and should be used especially when explaining good practice to younger pupils.

## 5. Filtering & Monitoring

5.1 In order to create a safe and productive digital learning environment, it is essential for all pupils to adhere to this policy. The School has implemented internet filtering and

monitoring measures to ensure that online content accessed during school hours aligns with educational objectives and maintains a secure environment.

5.2 The school's filtering system is designed to restrict access to inappropriate websites and content, including those that may be harmful or disruptive. Pupils are expected to use devices in School responsibly and refrain from attempting to bypass or tamper with the filtering settings.

5.3 Additionally, monitoring tools are in place to oversee all activities, fostering a sense of accountability and discouraging misuse of technology. By following these guidelines, pupils contribute to a positive and focused learning environment, fostering a culture of responsible digital citizenship within the school community.

5.4 Should a pupil have a concern regarding breach of this policy, they should contact the Director of Digital Strategy or Designated Safeguarding Lead who are responsible for filtering and monitoring within the School.

5.5 An attempt to access inappropriate websites or information will result in disciplinary action as per the Schools Behaviour Policy and/or legal action.

## **6. Google Workspace for Education**

6.1. Crosfields uses Google Workspace for Education to provide and manage a Google Workspace for Education account for pupils. Pupils must always use their Crosfields Google Workspace for Education account when accessing Google's services at the school.

6.2. Pupils must abide by Google's Terms of Service for all services provided as part of their Google Workspace for Education account.

6.3. Acceptance of the IT Acceptable Use Policy for Pupils includes parental consent for the School to maintain a Google Workspace for Education account for their child and for Google to collect, use, and disclose information about their child only for the purposes described in the [Google Workspace for Education Privacy Notice](#).

## **7. Long-term care and support of devices**

- 7.1. Pupils and their parents/guardians are solely responsible for the care and maintenance of their devices unless the device has been purchased as a service from the school.
- 7.2. Pupils must have current antivirus software installed on their device and must continue to maintain the latest service packs, updates, and antivirus definitions.
  - 7.2.1. The school highly recommends that pupils use [Microsoft Defender Antivirus](#) to ensure that their device remains fully compatible with our network.
- 7.3. Pupils are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.
- 7.4. Pupils are responsible for managing the battery life of their device. Pupils must ensure that their device is fully charged before bringing it to school. The school is not responsible for providing facilities for pupils to charge their device.
- 7.5. Pupils are responsible for backing-up their own data and should ensure that this is done regularly. Pupils should save their academic data using the Microsoft OneDrive cloud storage facility provided by the school.

## **8. Damage and loss**

- 8.1. Pupils are responsible for securing and protecting their device while at the school and while travelling to and from the school. This includes protective/carry cases and exercising common sense when storing their device.
- 8.2. Croxfields does not accept responsibility for theft, any damage or loss of a device or parts/accessories.
- 8.3. Pupils should clearly label their device for identification purposes. Labels should not be easily removable.

8.4. Pupils should read and understand the limitations of the manufacturer's warranty on their device, both in duration and in coverage.

## 9. Technical support

9.1. Pupils must download and install a copy of the suitable Impero Backdrop client on their BYOD device. The Impero Backdrop client must always be running and logged in while the pupil is present at the School.

9.2. Pupils must download and install a copy of Microsoft Office 365 on their BYOD device. The school will provide pupils with up to five Microsoft Office 365 licenses; these licenses can be used to install Microsoft Office 365 on up to five devices that are used within the pupil's home.

9.3. Pupils have the option to install a copy of the Adobe Creative Cloud applications on their BYOD device.

9.3.1. Please note that the 'Crosfields Minimum BYOD Device Requirements' do not meet the minimum system requirements for all Adobe Creative Cloud desktop applications.

9.3.2. Pupils will have the option to access all Adobe Creative Cloud desktop applications in the school's computing suites.

9.4. It may be necessary for pupils to install additional software depending on the course being taken. Please do not purchase any additional software for use within the school as this will be provided.

9.5. Pupils are responsible for the installation of any software on their device.

## 9.6. IT Help Desks

9.6.1. IT Help Desk services will centre on software application support and connectivity issues.

9.6.2. Any hardware or software problem that cannot be solved must be dealt with by the company from which the device was bought.

9.6.3. Where it becomes necessary to reinstall system or application software, pupil responsibilities as outlined in clause 8.5 apply.

## 9.7. BYOD loan devices

9.7.1. Loan devices may be available when hardware failures occur to BYOD devices purchased from a retailer. Pupils must provide the IT Help Desk with a repair agent receipt before a loan device can be issued for the duration of the repair.

9.7.2. If a loan device is not returned within the specified loan period, a device cost of £300.00 will be charged to the pupil's fee account.

# 10. Insurance

10.1. Pupil devices are not covered by Crosfields insurance. Insurance is the responsibility of parents/guardians and pupils.

# 11. Crosfields' Technology Standards

11.1. The School's Wi-Fi network operates on the 802.11ac 5 GHz standard. Devices that do not support this standard as a minimum will not be able to connect.

## 11.2. Device requirements

11.2.1. Pupil devices should meet the minimum requirements as outlined in the 'Crosfields Minimum BYOD Device Requirements' document.

11.2.2. Crosfields cannot guarantee that devices that do not meet the minimum requirements will be suitable for pupils to successfully engage in their learning.

## **12. Security and device management processes**

12.1. Pupils should protect their device using a strong password to access the operating system.

12.2. Microsoft recommends the following password complexity requirements:

12.2.1. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters.

12.2.2. Be at least 12 characters in length.

12.2.3. Contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, \$, #, %)

12.3. Pupils should not divulge their password (or anyone else's password) to any other person.

12.4. Pupils should only use their own network log-in details and should never share them with others. Any action using a user's password will be assumed to have been actioned by that user.

## **Appendix 1 – Pupil Acceptable usage policy in ‘Child Speak’**

### **Nursery, Reception and Year 1**

These are the rules I agree to follow when using any digital technology:

- \* I only go online with a grown up
- \* I only click on buttons when I know what they do
- \* I am kind online
- \* I keep information safe about me online
- \* I tell a grown up if something online makes me unhappy or worried

### **Years 2 to 4**

These are the rules I agree to follow when using any digital technology:

- \* I will only use ICT in school for school purposes
- \* I will only open attachments from people I know, or who my teacher has approved
- \* I will not tell other people my ICT passwords
- \* I will only open/delete my own files
- \* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- \* I will only take a photo or video of someone if they say it is okay
- \* I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
- \* I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- \* I will only change the settings on the computer if a teacher has allowed me to

- \* I know that my use of ICT can be checked, and my parent/carer contacted if a member of school staff is concerned about my safety
- \* I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- \* I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- \* I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about keeping safe online

### **Years 5 to 11**

These are the rules I agree to follow when using any digital technology:

- \* I always ask permission from an adult before using the internet
- \* I only use websites and search engines that my teacher has chosen
- \* I use my school computers for schoolwork unless I have permission otherwise
- \* I know that not everything or everyone online is honest or truthful and will check content on other sources like other websites, books or with a trusted adult
- \* I only talk with and open messages from people I know, and I only click on links if I know they are safe
- \* I always talk to an adult if I am not sure about something or if something happens online that makes me feel worried or frightened
- \* I only send messages which are polite and friendly
- \* I keep my personal information safe and private online
- \* I will keep my passwords safe and private as my privacy, schoolwork and safety must be protected
- \* I will not access or change other people's files or information
- \* I will only post pictures or videos on the Internet if they are appropriate and if I have permission.
- \* I know bullying in any form (online or offline) is not tolerated and I know that technology should not be used for harassment
- \* I will only change the settings on the computer if a teacher/technician has allowed me to

- \* I understand that the school's Internet filter is there to protect me, and I will not try to bypass it.
- \* I know that people I meet online may not always be who they say they are. If someone online suggests meeting up, I will immediately talk to an adult
- \* I know that my use of school computers and Internet access will be monitored
- \* If I see anything online that I should not or that makes me feel worried or upset then I will minimise the page and tell an adult straight away
- \* I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- \* I can visit [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) and [www.childline.org.uk](http://www.childline.org.uk) to learn more about keeping safe online
- \*I will only use devices when supervised by a member of staff
- \*I will not use my BYOD device during break or lunchtimes (Years 7 to 9)

## **Appendix 2 – E-mail Etiquette**

### **Email Etiquette**

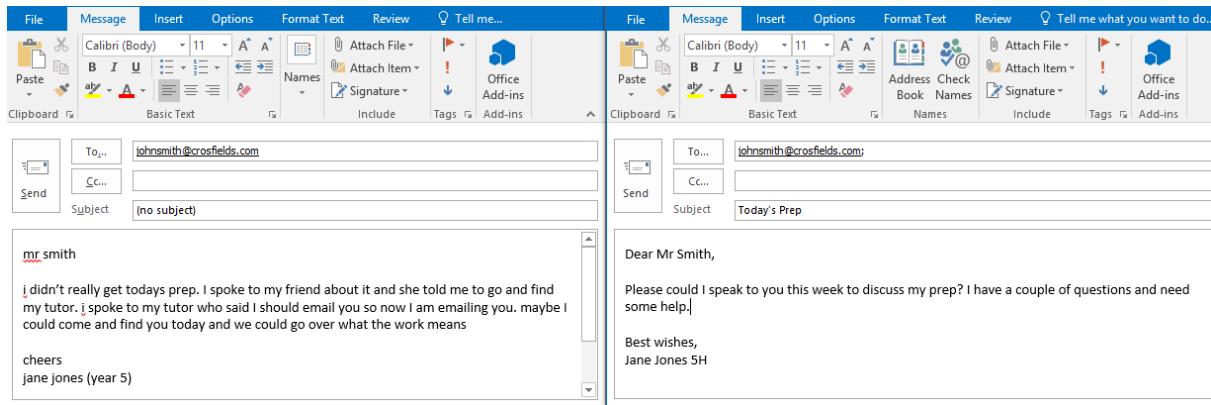
Pupils from Year 5 will be able to use Crosfields' email system. Email is short for electronic mail i.e. a digital letter. Authoring an email is like writing a letter, so some of the same rules should be followed. I agree to follow these rules when using the school's email system:

#### **Before Sending an Email...**

1. Is an email necessary? Could you speak to that person face-to-face instead? If your email requires an urgent reply, face-to-face is often better. If you are emailing a teacher, please give them at least 24 hours to respond to your email.
2. During lesson time, you should not be using email to communicate with classmates unless given permission to do so by your teacher. Please only use the school email for communicating with **@crosfields.com** email addresses.
3. Emails sent and received at Crosfields are monitored for inappropriate content. This is for your safety. If something upsets you or makes you feel uncomfortable, please talk to a trusted adult e.g. parent or teacher.
4. The repeated sending of unkind emails is called cyberbullying. This is not acceptable at Crosfields. Emails are monitored so please do not do this. If this is happening to you, please find a trusted adult who can help you.

#### **While Sending an Email...**

5. All emails should have a subject line (heading) that uses capital letters correctly. The subject line should tell you what the email is about.
6. In the main body of text, start with a greeting. If you are emailing teachers, please use their titles e.g. Mr, Miss, Ms or Mrs.
7. The body of the email is where the message goes. Keep your message to the point.
8. At the end of the email, sign off with an appropriate ending, saying who you are.



***Please see above for an example of a badly written email compared with a well-written one.***

### **Before Pressing Send...**

9. If you think you have finished your email, double-check spelling, punctuation and grammar. Writing everything in upper-case is not appropriate as it suggests you are shouting. Writing everything in lower-case looks careless and that you have not put any thought into what you have written.
10. Double check you have inserted an attachment to an email.
11. If you are happy that the email is appropriate and has been proof read, press send

