GORDON’S SCHOOL

SAFE USE OF TECHNOLOGY POLICY

The core principle that guides everything we do is **Putting Students First.**

This document recognises the School’s commitment to online-safety. The document develops a set of acceptable behaviours that enable the School to reduce risks whilst continuing to benefit from IT hardware, software and systems that are available to enhance learning. This document is comprised of the following policies that promote the safe use of technology at Gordon’s;

A. Online-safety Policy

B. Acceptable Use of Mobile Devices Policy

C. Staff Social Media Policy

D. Bring Your Own Device (BYOD) Policy

Appendix I. Acceptable Use of IT Policy – Staff Declaration

Appendix II. Acceptable Use of IT Policy – Guest Declaration

Appendix III. Acceptable Use of IT Policy – Student Declaration

Appendix IV Acceptable Use of IT Policy – Parent / Carer Declaration

For the purposes of this policy, “school” refers to Gordon’s School, both the Academy and the Gordon Foundation. “Staff” refers to all employees, volunteers, governors, trustees, contractors, peripatetic teachers, coaches and tutors, helpers and any other adult serving the Academy or the Gordon Foundation.

Helen Carruthers
Deputy Head (Pastoral)

Jane Valmer
Chair of Governors and Safeguarding Governor

September 2023

A. Online-safety

Online-safety is part of the school's safeguarding responsibilities. Please see also;

- Behaviour Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Cyber-bullying Policy
- Data Protection Policy

Using this policy

i. The School has an online-safety committee and an online-safety co-ordinator.

ii. This online-safety policy has been written by the School, building on best practice and government guidance. It has been agreed by SLT and approved by Governors.

iii. The online-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school premises. This includes but is not limited to workstations, laptops, mobile devices, tablets and hand held games consoles used on the school premises.

iv. The online-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / student.

The online-safety Committee

i. The Committee comprises of;

   a. The online-safety co-ordinator

   b. 1 member of SLT

   c. The Assistant Bursar

   d. 1 member of Residential House staff

   e. 1 member of Day House staff

   f. 1 member of IT teaching staff

   g. 1 member of support staff

   h. 1 representative from the service provider

ii. The committee will meet once per term to review and share information about online-safety issues.

iii. The Safe Use of Technology Policy will be reviewed annually.

The online-safety co-ordinator

The online-safety coordinator will:

i. Complete the online-safety audit (see E-safety Toolkit at www.surreycc.gov.uk) in conjunction with the Wider Leadership Team

ii. Promote an online-safe culture under the direction of the Senior Leadership Team, and promote the School's online-safety vision to all stakeholders

iii. Maintain the School's online-safety policy, reviewing it annually

iv. Ensure that the online-safety policy links with other appropriate school policies e.g. Anti-Bullying, Safeguarding, PSHE etc. (with the appropriate members of staff)

v. Ensure the online-safety policy and its associated practices are adhered to (e.g. incident flow charts, reporting logs etc.)

vi. Ensure Acceptable Use Policies/school internet rules are in place, up-to-date and wherever possible are agreed by Staff, Students and Parents

vii. Work with the SENCO and Designated Safeguarding Lead to create online-safety guidance for vulnerable children and those with additional learning needs

viii. Manage online-safety training for all staff and ensure that online-safety is embedded within continuing professional development

ix. Ensure staff receive relevant information about emerging issues

x. Coordinate online-safety awareness raising/education for students and ensure that online-safety is embedded in the curriculum, for example via online-safety schemes of work, assemblies and/or theme days

xi. Support online-safety awareness raising/education initiatives for parents

xii. Act as a point of contact, support and advice on online-safety issues for staff, students and parents

xiii. Act as the first point of contact should an online-safety incident occur (particularly child protection or illegal issues), and ensure the agreed online-safety incident procedure is followed, as outlined in the School's online-safety policy

xiv. Maintain an online-safety incident log

xv. Monitor, report and address incidences of students accessing unsuitable sites at school as necessary

xvi. Keep up-to-date with local and national online-safety awareness campaigns and issues surrounding existing, new and emerging technologies

xvii. Work with and receive support and advice from the SSCB online-safety sub-group and where necessary, the Police.

Managing access and security

i. The school will provide managed internet access to its staff and students in order to help students to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

ii. The school will use a recognised internet service provider or regional broadband consortium.

iii. The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.

iv. The school will ensure that its networks have virus and anti-spam protection.

v. Access to school networks will be controlled by personal passwords.

vi. Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept by the Deputy Head (Pastoral) to help to identify patterns of behaviour and to inform online-safety policy.

vii. The security of the School's IT systems will be reviewed termly.

viii. All staff who manage filtering systems or monitor IT use will be supervised by SLT and have clear procedures for reporting issues.

ix. The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

i. The school will provide an age-appropriate online-safety curriculum that teaches students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

ii. All communication between staff and students or families will take place using school hardware and/or school accounts.

iii. Students will be advised not to give out personal details or information which may identify them or their location

E-mail

i. Students and staff may only use approved e-mail accounts on the school IT systems.

ii. Staff to student email communication must only take place via a school email address or from within the learning platform.

iii. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

iv. The School will monitor how e-mail from students' school accounts to external bodies is presented and controlled.

Published content (eg school website, school social media accounts)

i. The contact details will be the school address, email and telephone number. Private information will not be published.

ii. The Head Teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

i. Parents will receive information about our Taking Images of Children Policy in the School's Joining Pack. The policy asks parents to contact the School only if they object to having their child's photograph taken. Parental permission will be sought if the School is using an individual image in an article with the student's first and last names (but not if it is solely their first name).

Use of social media including the school learning platform

i. The school will control access to social networking sites and consider how to educate students in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

ii. Use of video services such as Skype, Teams, Google Hangouts and Facetime will be monitored by staff in Residential Houses and provision will be made for Residential Boarders to contact friends and family by these means.

iii. Staff and students should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

i. Personal equipment may be used by staff and/or students to access the school IT systems provided their use complies with this Safe Use of Technology Policy and the relevant AUP (Acceptable Use Policy) below.

ii. Staff must not store images of students or student personal data on personal devices.

iii. The school cannot be held responsible for the loss of, or damage to, any personal devices used in school or for school business.

Online-safety rules and sanctions

It is appropriate for people to be allowed a great deal of freedom in using IT for study, work and leisure. With freedom comes responsibility. Gordon's School cannot control what people, all over the world, make available on the internet; a small proportion of the material which it is possible to access is not acceptable in school, whilst other material must be treated with great sensitivity and care. Exactly the same standards apply to electronic material, as to material in any other form.

We expect all IT users to take responsibility in the following ways:

i. Not to access or even try to access any material which is:

   a. Violent or that which glorifies violence

   b. Criminal, terrorist or glorified criminal activity (including drug abuse)

   c. Racist or designed to incite racial hatred

   d. Of extreme political opinion

   e. Pornographic or with otherwise unsuitable sexual content

   f. Crude, profane or with otherwise unsuitable language

   g. Blasphemous or mocking of religious and moral beliefs and values

   h. In breach of the law, including copyright law, data protection, and computer misuse

   i. Belongs to other users of IT systems and which they do not have explicit permission to use

ii. Not to search for, or use websites that bypass the school's internet filtering

iii. Not to download or even try to download any software without the explicit permission of a member of the IT systems support department

iv. Not to attempt to install any unauthorised or unlicensed software

v. To be extremely cautious about revealing any personal details and never to reveal a home address or mobile telephone number to strangers

vi. Not to use other people's user ID or password, even with their permission

vii. Not to interfere with or cause malicious damage to the IT facilities

viii. To report any breach (deliberate or accidental) of this policy to a member of staff immediately.

In order to protect responsible users, electronic methods will be used to help prevent access to unsuitable material. Gordon's School reserves the right to access all material stored on its IT system, including that held in personal areas of staff and student accounts for purposes of ensuring DfE, Local Authority and school policies regarding appropriate use, data protection, computer misuse, child protection, and health and safety. Anyone who is found not to be acting responsibly in this way will be disciplined. Irresponsible users will be denied access to the IT facilities. Gordon's School will act strongly against anyone whose use of IT risks bringing the school into disrepute or risks the proper work of other users. Persistent offenders will be denied access to the IT facilities on a permanent basis.

Sanctions for the misuse of Gordon's School IT facilities

Note: Depending on the severity of the offence these steps may be bypassed to the appropriate level. In the case of staff misuse, the school's disciplinary procedures will be used.

First Offence

i. The student will have a School Detention, set by the online-safety co-ordinator, after discussing the breaking of the IT AUP.

ii. The student will need to read the IT AUP to ensure they are clear about the regulations by the completion of an educational worksheet.

iii. The relevant Head of House will inform parents of the breaking of the IT AUP.

iv. The student may receive a further sanction depending on the nature of the offence.

v. The Deputy Head (Pastoral) will be informed.

vi. The incident and response will be logged on SIMS.

Second Offence

i. The Deputy Head (Pastoral) will write a letter to parents and phone them to inform them of the breaking of the IT AUP for the second time. The letter may include specific information about the offence.

ii. The student will have restrictions placed on their use of the IT facilities by the removing of email and/or internet access for a period of time.

iii. The student may receive a further sanction depending on the nature of the offence.

iv. The relevant Head of House will be informed.

v. The incident and response will be logged.

Third Offence

i. The student will have their email and/or internet access removed immediately by the Deputy Head (Pastoral) for up to 3 weeks.

ii. The Deputy Head (Pastoral) will write a letter to parents and phone them to inform them of the breaking of the IT AUP for the third time. The letter will ask parents to come into school to discuss the breaking of the IT AUP with the Deputy Head (Pastoral).

iii. The student will have a meeting with the Deputy Head (Pastoral) to discuss the breaking of the IT AUP and the subsequent sanction.

iv. The relevant Head of House will be informed.

v. The incident and response will be logged.

Fourth Offence

i. The student will have all access to the Gordon's School network removed until further notice.

ii. The student will be banned from accessing IT hardware in the school unless supervised directly by a teacher.

iii. The Head Teacher will write a letter to parents and phone them to inform them of the breaking of the IT AUP for the fourth time. The letter will ask parents to come into school to discuss the breaking of the IT AUP with the Head Teacher.

iv. The student will have a meeting with the Head Teacher and Deputy Head (Pastoral) to discuss the breaking of the IT AUP and the subsequent sanction, which may involve a form of exclusion depending on the nature of the infringement.

v. The relevant Head of House will be informed.

vi. The incident and response will be logged.

vii. It should be noted that if a student puts themselves, other students or a member of staff in danger by giving out personal details they will be banned from using the IT facilities for a fixed period of time and if required the police will be informed.

Protecting personal data

The school has a separate Data Protection Policy. It covers the access to student and staff personal data on and off site, and remote access to school systems.

Authorising access

i. All staff (including teaching assistants, support staff, office staff, student teachers, work experience trainees, IT technicians and governors) must read and sign the 'Staff AUP (Acceptable Use Policy)' before accessing the school IT systems.

ii. The school will maintain a current record of all staff and students who are granted access to school IT systems.

iii. All students must apply for internet access individually by agreeing to comply with the student AUP.

iv. People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or for any consequences this material may affect.

Handling online-safety complaints

i. Complaints of internet misuse will be dealt with in accordance with this policy.

ii. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

iii. Students and parents will be informed of consequences and sanctions for students misusing the internet in accordance with this policy.

Community use of the internet

Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school online-safety policy.

Communication of the Policy

To students:

Students need to agree to comply with the student AUP in order to gain access to the school IT systems and to the internet

Students will be reminded about the contents of the AUP as part of their online-safety education

To staff:

All staff will be shown where to access the online-safety policy and its importance explained.

All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet

All staff will receive online-safety training on an annual basis

To parents:

The school will ask all new parents to sign the parent /student agreement when they register their child with the school.

Parents' and carers' attention will be drawn to the Safe Use of Technology Policy in newsletters, the school brochure and on the school website. Parents will be offered regular online-safety information through information evenings and weekly schoolcomms..

B. Acceptable Use of Mobile Devices Policy

Definition

For the purpose and interpretation of this policy, ‘mobile devices’ and ‘personally-owned mobile devices’ include electronic tablets or similar such devices that have been supplied by the school but which are owned by the student and which have been, or are being paid for by the student’s family under a standard financial agreement with the school or by any other such financial arrangement including bursarial support or pupil premium arrangements.

Purpose

i. The widespread ownership of mobile devices among young people requires that school administrators, teachers, students, parents and carers take steps to ensure that mobile devices are used responsibly at school. This Acceptable Use of Mobile Devices Policy is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that mobile devices provide (such as increased safety) can continue to be enjoyed by our students.

ii. Gordon’s School has established the following Acceptable Use Policy for mobile devices that provides teachers, students, parents and carers guidelines and instructions for the appropriate use of mobile devices during school hours.

iii. Students, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile devices to school.

iv. The Acceptable Use Policy for mobile devices also applies to students during school excursions, camps and extra-curricular activities both on the school campus and off-site.

Rationale

The school recognises that personal communication through mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately and safely.

Personally owned mobile devices include phones, smart watches, tablets, laptops or any device capable of accessing the internet or transferring digital information to other people, other than a student’s ***school-issued*** tablet / device.

General use of personally owned mobile devices

i. Personally owned mobile devices brought into school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally owned mobile devices, irrespective of whether or not the student is using it as part of a lesson.

ii. Mobile devices and personal devices are not permitted to be used in certain areas within the school site such as changing rooms and toilets.

iii. Mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with explicit consent from a member of staff.

iv. The Bluetooth functionality of a mobile device should be switched off at all times and may not be used to send images or files to other mobile devices.

v. No images or videos should be taken on mobile devices or personally owned mobile devices without the prior consent of the person or people concerned.

Students' use of personally owned mobile devices

i. If a student breaches the school policy then the device will be confiscated and will be held in a secure place in the School Office. Mobile devices will be released either to students, to parents or carers of Day Boarders, or to Houseparents of Residential Boarders at the end of the school day.

ii. Devices must not be taken into examination rooms. Students found in possession of a mobile device during an examination will be reported to the appropriate examining body. This may result in the withdrawal of the student from either that examination or all examinations.

iii. Parents are advised not to contact their child via their mobile device during the school day, but to contact the School Office or House office.

iv. Students should protect their device numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile devices and personal devices and will be made aware of boundaries and consequences and encouraged to use PINs and other security as necessary.

v. Students may be provided with school mobile devices to use in specific learning activities under the supervision of a member of staff. Such mobile devices will be set up so that only those features required for the activity will be enabled as necessary.

Staff use of personally-owned mobile devices

i. Staff will be issued with a school device where contact with students, parents or carers is required, for example a mobile on school trips or staff-based landline in departments or school offices. Where staff members are required to use a mobile device for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile device will be provided and used. In an emergency where the staff member doesn't have access to a school owned device, they should use their own devices and hide (by inputting 141 or blocking Caller ID) their own mobile numbers for confidentiality purposes.

ii. Mobile devices and personally owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile devices must not be used during teaching periods unless permission has been granted by a member of the senior leadership team, or in emergency circumstances.

iii. Staff must not store photos or videos of students on their privately owned devices and will only use school provided equipment for this purpose.

iv. If a member of staff breaches the school policy, then disciplinary action may be taken as appropriate.

v. Staff use of mobile devices during the school day will normally be limited to non-contact times of the school day.

vi. Staff should ensure that their devices are protected with PIN/access codes in case of loss or theft.

vii. Staff should not send and read texts in classrooms or use camera devices at any time unless part of a teaching or learning process.

viii. Staff should never contact students from their personal mobile device or give their mobile device number to students. If a member of staff needs to make telephone contact with a parent, a school telephone should be used.

ix. Staff should never store parents' or students' telephone or contact details on their mobile device, as this allows the possibility of inappropriate contact.

x. Staff should never send, or accept from anyone, texts or images that could be viewed as inappropriate.

xi. If a member of staff suspects a message, text or similar may contain inappropriate content it should not be opened but a senior member of staff, preferably the online-safety coordinator or DSL should be contacted.

Personal safety and security

The School accepts that parents/carers may give their children mobile devices to protect them from everyday risks involving personal security and safety. There is also increasing concern about children travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile device gives parents reassurance that they can contact their child if they need to speak to them urgently.

Responsibility

i. It is the responsibility of students who bring mobile devices to school to abide by the guidelines outlined in this document.

ii. The decision to provide a mobile device to their children should be made by parents or carers. It is incumbent upon parents to understand the capabilities of the device and the potential misuse of those capabilities.

iii. Parents/carers should be aware that if their child takes a mobile device to school it is assumed household insurance will provide the required cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.

iv. Students are responsible for keeping the school informed of their current mobile device to aid return if lost on the school premises.

v. Parents/carers are reminded that in cases of emergency, the House or School Reception remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any relevant way. Passing messages through the House or School Reception also reduces the likelihood of disrupting lessons inadvertently.

Acceptable Uses

i. Mobile devices will be switched off (not just put on silent mode) and will be kept out of sight during classroom lessons, school assemblies and Chapel services, whilst moving between classrooms and when in the library.

ii. Students are only permitted to use mobile devices in classrooms with permission, in the Library, on the Parade Square and Front Field (but not between lessons) and in designated areas in Houses.

iii. Parents/carers are requested that in cases of emergency they contact the House or School Reception first. This ensures that staff are aware of any potential issue and may make the necessary arrangements.

iv. Mobile devices should not be used in any manner or in any location that could cause disruption to the normal routine of the school.

v. Students should protect their device numbers and social media access by giving access details only to close friends and family. This will help protect the student's details from falling into the wrong hands and guard against insulting, threatening or unpleasant communications.

vi. The school recognises the importance of emerging technologies present in modern mobile devices e.g. camera and video recording, internet access, MP3 and MP4 playback, blogging etc. Teachers may wish to utilise these functions to aid teaching and learning and students may have the opportunity to use their mobile devices in the classroom. On these occasions, express permission will be given by the teacher. Students may then use their mobile devices in the classroom for that lesson only. The use of personal mobile devices in one lesson for a specific purpose does not mean further usage is then acceptable.

vii. If asked to do so, students must show the content requested or hand their device to a member of staff or other designated adult including the police.

Theft or damage

i. The responsibility for keeping a student's mobile device safe lies with the student; the school accepts no responsibility for replacing lost, stolen or damaged mobile devices.

ii. The school accepts no responsibility for students who lose or have their mobile devices stolen while travelling to and from school.

iii. Students should mark their mobile device clearly with their name or an identifiable detail.

iv. Students in Y7-11 who bring a mobile device to school should hand it in to the house office. 6th Form may keep their phones during the day but they should be out-of-sight in classrooms, the dining hall and when walking around school.

v. To reduce the risk of theft during school hours, students who carry mobile devices are advised to keep them well concealed and not 'advertise' that they have them.

vi. When a mobile device is found on the school premises and the owner cannot be located, it should be handed into the School Office.

vii. It is strongly advised that students use passwords and/or pin numbers to ensure that unauthorised communications cannot be made on their devices (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile devices and/or passwords must not be shared.

viii. Lost and stolen mobile devices in the U.K. can be blocked across all networks making them virtually worthless to the thief. Call your network provider as soon as possible after your device has been lost or stolen. This can be a temporary measure in case it is recovered.

Inappropriate conduct

i. Using mobile devices to bully or threaten students or staff is unacceptable. Cyberbullying will not be tolerated. In some cases it could constitute criminal behaviour. Using technology to humiliate, embarrass or cause offence will not be tolerated; regardless of whether 'consent' was given.

ii. It is forbidden for students to use their own or other students' mobile devices to take videos and pictures of acts to denigrate or humiliate others. This also includes using mobile devices to photograph or film any student or member of staff without their consent. It is a criminal offence to use a mobile device to menace, harass or offend another person; almost all communications can be traced.

iii. Mobile devices are not to be held or used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to other students, staff or visitors to the school.

iv. Should there be any disruption to lessons caused by a mobile device, the responsible student may face disciplinary actions as sanctioned by the Head Teacher. This may include a mobile device ban in school for one, some or all students.

v. It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the student will be asked and instructed to delete those images.

vi. Mobile devices are banned from all examinations. Students MUST hand devices to invigilators before entering the exam hall. Any student found in possession of a mobile device during an examination may have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

vii. Any student who uses vulgar, derogatory, or obscene language while using a mobile device will face disciplinary action.

viii. Students may not engage in personal attacks, harass another person, or post private information using any form of IT. Students using mobile devices to bully other students will face disciplinary action.

ix. Students must ensure that files stored on their devices do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence. Similarly, ‘sexting’ – which is the sending of personal sexual imagery - is a criminal offence.

Sanctions

i. Students who infringe the rules set out in this document could face having their devices confiscated by teachers. If the device is being used inappropriately the student must give it to a teacher if requested.

ii. On any infringement of this policy the mobile device will be confiscated by the teacher and taken to a secure place within the School Office. The student will be able to collect the mobile device at the end of the school day from their House and a record will be made of the incident.

iii. If a device is used by a student or member of staff such that the action raises a safeguarding concern, it will be reported to the DSL who may make a further referral to SSCB.

iv. If a device is used by a student or member of staff to commit a criminal act, including a breach of the Malicious Communications Act, then the police will be informed.

C. Staff Social Media Policy

Introduction

i. The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

ii. While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that staff are expected to follow when using social media.

iii. It is crucial that students, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of students and other staff and the reputation of the school are safeguarded.

iv. Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

i. For the purposes of this policy, "school" refers to Gordon's School, both the Academy and the Gordon Foundation. "Staff" refers to all employees, volunteers, governors, trustees, contractors, peripatetic teachers, coaches and tutors, helpers and any other adult serving the Academy or the Gordon Foundation.

ii. This policy covers personal use of social media as well as the use of social media for official school purposes, including sites hosted and maintained on behalf of the school (see below).

iii. This policy applies to personal webspace such as social networking sites (for example *Facebook*), blogs, microblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal Framework

i. Gordon's School is committed to ensuring that all staff members provide services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

ii. Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- School or business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
- Politically sensitive information.

iii. Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

iv. Gordon’s School could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Gordon’s School liable to the injured party.

Principles

i. You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school and your personal interests.
ii. You must not engage in activities involving social media which might bring Gordon’s School into disrepute.
iii. You must not represent your personal views as those of Gordon’s School on any social medium.
iv. You must not discuss personal information about students, school staff and other professionals you interact with as part of your job on social media.
v. You must not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations, or Gordon’s School.
vi. You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Gordon’s School.

Personal use of social media

i. Staff members must not have contact through any personal social medium with any student, whether from Gordon’s School or any other school, unless the students are family members.
ii. Gordon’s School does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.
iii. Staff members must not have any contact with students’ family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.
iv. If staff members wish to communicate with students through social media sites or to enable students to keep in touch with one another, they can only do so with the approval of SLT and through official school sites created according to the requirements specified in this policy.
v. Staff members must decline ‘friend requests’ from students and parents of students they receive in their personal social media accounts. If they receive such requests from students who are not family members, they must discuss these in general terms in class and signpost students to become ‘friends’ of the official school site.
vi. On leaving the school’s service, staff members must not contact Gordon’s students by means of personal social media sites. Similarly, staff members must not contact students from their former schools by means of personal social media.
vii. Information staff members have access to as part of their employment, including personal information about students and their family members, colleagues, and other parties and school corporate information must not be discussed on their personal webspace.
viii. Photographs, videos or any other types of image of students, unless family members, or images depicting staff members wearing clothing with school logos or images identifying school accommodation must not be published on personal webspace.

ix. School email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

x. Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

xi. The school's corporate, service or team logos or brands must not be used or published on personal webspace.

xii. Gordon's only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not allowed during contact times.

xiii. Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships.

xiv. Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information.

Using social media which represents Gordon's School

i. Staff members must only use official school sites for communicating with students or to enable students to communicate with one another.

ii. There must be a strong pedagogical or business reason for creating official school sites to communicate with students or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.

iii. Official school sites must be created only according to the requirements specified in this policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

iv. Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

Creating social media sites on behalf of Gordon's School

i. Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of the School.

ii. Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical or pastoral outcome.

iii. The proposed audience and level of interactive engagement with the site, for example whether students, school staff or members of the public will be able to contribute content to the site, must be discussed with the Deputy Head (Pastoral).

iv. Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

v. The site-owner must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

vi. There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image.

vii. Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

Student consideration

i. When creating social media sites for students and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.
ii. When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.
iii. If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.
iv. Staff members must ensure that the sites they create or contribute to for work purposes conform to the Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services (Home Office Task Force on Child Protection on the Internet, 2008)
v. Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.
vi. Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.
vii. Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from the Deputy Head (Pastoral).

Approval for creation of or participation in webspace

i. Gordon's School's social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Gordon's employees or other authorised people.
ii. Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the staff member's line manager, the Deputy Head (Pastoral) or the Head Teacher.
iii. Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager and the Deputy Head (Pastoral).
iv. The Deputy Head (Pastoral) must be consulted about the purpose of the proposed site and its content. In addition, SLT approval must be obtained for the use of the school logo and brand.
v. Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Head Teacher immediately. Staff members must not communicate with the media without the advice or approval of the Head Teacher.

Content of webspace

i. Gordon's-hosted sites must have clearly expressed and publicised Terms of Use. Third-party hosted sites used for work purposes must have Terms of Use that conform to the school's standards of professional conduct and service.
ii. Staff members must not disclose information, make commitments or engage in activities on behalf of Gordon's School without authorisation.
iii. Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the School's image, reputation and services.
iv. Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.
v. Staff members must respect their audience and be sensitive in the tone of language used when discussing topics that others may find controversial or objectionable.

vi. Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

vii. Gordon's-hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website.

viii. Staff members participating in Gordon's-hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites.

ix. Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

x. Personal opinions must not be expressed on official sites.

Contributors and moderation of content

i. Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

ii. Sites created for and contributed to by students must have the strongest privacy settings to prevent breaches of confidentiality. Students and other participants in sites must not be able to be identified.

iii. The content and postings in Gordon's-hosted sites must be moderated. Moderation is the responsibility of the department that sets up or initiates the site.

iv. The department must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removing comments which breach the terms of acceptable use. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

v. For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.

vi. Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

vii. Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with minimum expectations of decency and appropriacy must not be posted or removed.

viii. Approval must also be obtained from the Deputy Head (Pastoral) to make an external organisation a 'friend' of the site.

Monitoring of internet use

i. Gordon's School monitors usage of its internet and email services without prior notification or authorisation from users.

ii. Users of Gordon's School's email and internet services should have no expectation of privacy in anything they create, store, send or receive using the school's IT system.

Breaches of the policy

i. Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Gordon's School's disciplinary procedures.

ii. A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Gordon's School or any illegal acts or acts that render Gordon's School liable to third parties may result in disciplinary action or dismissal.

iii. Contracted providers of services must inform the School immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the School. Any action against breaches should be according to contractors’ internal disciplinary procedures.

D. BYOD Policy

Purpose

The School recognizes the convenience of students using their own devices for educational purposes and this policy is intended to enable this to happen safely and positively.
This policy is to be read in conjunction with Section B. Acceptable Use of Mobile Devices Policy in respect to the acceptable use of privately owned devices in school.

Key Stage 3 & 4 Students

Key Stage 3 & 4 students are not permitted to bring mobile devices (eg smart phones, tablets etc) to school, other than their school-issued electronic tablet. If parents wish their child to carry an additional mobile device with them to and from school, then that device must be handed in to the House office upon arrival and collected at the end of the day.

Residential Boarders in Key Stage 3 & 4 may have their mobile devices in school, stored securely in their House. They may have access to their devices after prep in the evening until bedtime, and at weekends except overnight.

Key Stage 5 Students

- Use of personal devices on school grounds is at the discretion of teachers and staff. All students MUST use their devices as directed by their teacher and staff.
- The school provides secure facilities for students to store their personal devices. Students should keep their devices with them at all times if not locked in their secure area.
- The use of personal devices is not to be a distraction in the classroom or private study areas used by teachers or students.
- The purpose of the use of personal devices in the classroom is <u>strictly educational</u>. Mobile devices can only be used for personal reasons if the student has been given permission by a teacher or another member of staff.
- All users agree not to exploit technology resources, interfere with another student’s use of the resources, or use technology resources with the intent of causing harm to others.
- All students are required to check their personal devices daily to make certain the device is fully charged, free from unsuitable material and any malicious content such as viruses and malware that may compromise the security of the school’s network. These checks must be completed <u>before</u> bringing the device to school.
- To conform to Health and Safety compliance, any defective or damaged devices should not be brought into the school.
- Any attempt to circumvent the schools network security and/or filtering policies is forbidden. This includes downloading programs to bypass security or accessing and setting up proxies.
- Students are not allowed to use personal devices during the morning break.
- Any form of distribution of videos or pictures of other students and staff is strictly forbidden.
- Playing games on devices is NOT permitted unless the game is used for educational purposes.

Consequences for disruption and misuse.

In the event of any misuse of a device;

- Access to the school network and any accompanying privileges will be revoked (wireless and wired).
- Breach of any rules may result in the personal device being confiscated. The device will be returned to the student at the end of the school day by House staff before the student signs out to go home.
- For repeated offences and on the third infringement within one term, the student may be banned from using personal devices at school for a period of time that is at the discretion of the Deputy Head (Pastoral) and which will normally be 6 weeks.
- In certain more serious situations or for repeated offences, a student may be banned from using their own device in school at any time.

School Liability statement.

- It is the student's responsibility to ensure that their personal device is kept up to date with the latest operating system updates and upgrades.
- It is the student's responsibility to ensure that their device is kept secure. Every student personal device must be password protected. Additionally, the appropriate security software must be installed to protect personal devices against the latest malicious threats such as viruses, malware, etc.
- Parents are required to have adequate insurance coverage in place to cover the cost of replacement or repair of the student's personal device in the event of loss or damage that occurs on school premises, or during school visits and activities.

Please note, the School is **will not accept any liability** for the following:

- Any personal mobile device that is broken on school premises or during school visits and outside activities.
- Any personal devices that are stolen or lost on school premises or during school visits and outside activities.
- Any personal data that is lost on personal devices while they are being used on school premises.

User agreement

By signing the School's Acceptable Use of IT Policy – Student Declaration / Parent declaration, you agree to the following.

Students:

You agree not to connect to any other wireless or network service that is outside of the school network when using your personal device on school premises, or when taking part in school events and school activities.

By using your own personal device in the school or during school visits and school activities, you agree that you understand the school's Bring Your Own Device Policy (BYOD) and that you agree to be bound to the rules, regulations and statements contained in this BYOD Policy.

You also understand that the use of a personal device in school or for school activities is for learning purposes only and that it is a privilege, not a right to use your own personal device at school.

You understand that you are fully responsible for the safety, security and care of your personal device when using it in school, during school visits and participation in outside activities.

Parents:

You understand that Gordon’s School accepts no liability for any loss and/or damage to your children’s personal devices that are used in school, during school visits and activities, or when in transit to and from the school.

You understand that the decision to bring a personal device into the school rests with the parent/guardian, as does the liability for any loss and/or damage that may occur as a result of using the personal device in school, during school visits and other outside activities.

You understand that by allowing the student to bring their personal device into school, both you and the student agree to these terms and conditions and agree to be bound to the rules, regulations and statements contained in this BYOD Policy.

Appendix I.
Acceptable Use of IT Policy – Staff Declaration

i. IT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of IT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the online-safety coordinator.

ii. I appreciate that IT includes a wide range of systems, including mobile devices, tablets, digital cameras, email, social networking and that IT use may also include personal IT devices when used for school business.

iii. I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.

iv. I will only use the School's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head teacher or Governing Body.

v. I will comply with the IT system security and not disclose any passwords provided to me by the School or other related authorities.

vi. I understand that I am responsible for all activity carried out under my username.

vii. I will only use the approved, secure email system(s) for any school business.

viii. I will ensure that all electronic communications with parents, students and staff, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

ix. I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher or Governing Body.

x. I will only take images of students and/or staff for professional purposes in line with school policy.

xi. I will not install any hardware or software.

xii. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.

xiii. I will respect copyright and intellectual property rights.

xiv. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head Teacher.

xv. I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. I will support the School's online-safety policy and help students to be safe and responsible in their use of IT and related technologies. I will promote online-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. I will report any incidents of concern regarding children's safety to the online-safety coordinator, the Designated Safeguarding Lead or Head Teacher.

xvi. I understand that sanctions for disregarding any of the above will be in line with the School's disciplinary procedures and serious infringements may be referred to the police.

xvii. I understand that I may voluntarily declare the names of any persons under 19 years of age with whom I am in contact via social media, and that this information will be kept confidentially by the School.

Staff Signature

I agree to follow the Acceptable Use Policy and have understood and agree with the content of the Safe Use of Technology Policy.

Please tick one of the following

□ I wish to declare below the names and the relationship of Under 19s, excluding family members, with whom I am connected through social media. For example, AN Other / Sports club member

□ I do not wish to declare the names and the relationship of Under 19s with whom I am connected through social media.

□ I am not, to my knowledge, connected with any Under 19s through social media.

NAME	**RELATIONSHIP**
Please attach additional sheet if necessary	

Full Name… ………………………………………………… ……………………………

Job title …………………………………………………………………………………

Signature…. ….……………………… Date ………………………………..

Appendix II.

Acceptable Use of IT Policy – Guest Declaration

i. I understand that I have been given limited use of the school internet and/or school IT systems as a temporary guest user.

ii. I understand that it is a criminal offence to use a school IT system for a purpose not permitted by its owner.

iii. I will only use the school's email / internet / intranet / Learning Platform and any related technologies for the purpose for which I have been given access.

iv. I will comply with the IT system security and not disclose any passwords provided to me by the school or other related authorities.

v. I will not install any hardware or software.

vi. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory whilst using the school IT systems.

vii. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher or my employer.

viii. I will respect copyright and intellectual property rights.

ix. I understand that if I disregard any of the above then it will be reported to my employer and serious infringements may be referred to the police.

Name ………………………………………………………………………

Company ………………………………………………………………………

Signed …………………………

Date ………………………….

Appendix III.

Acceptable Use of IT Policy – Student Declaration

i. I know that school owns the computer network and there are rules on how I use it. I know that it would be against the law to use a computer or network for a reason which is not allowed by the school.

ii. I will only use IT systems in school, including the internet, email, digital video, mobile technologies, etc., for school reasons. I will not use IT systems at school for private reasons, unless the Head Teacher has given specific permission

iii. I will not use IT systems at school to make money for me, gambling, political activity, advertising or for activities which are against the law.

iv. I will only log on to the school network or learning platform with my own user name and password.

v. I accept that I am responsible for all activity carried out under my username. I accept that I am responsible for all activity by my user name.

vi. I will follow the School's IT rules and not reveal my passwords to anyone and change them often.

vii. I will only use my school email address for school work.

viii. I will make sure that all IT I share with students, teachers or others is responsible and sensible. I know that emails might be shared with people I did not send them to.

ix. I will not send messages without my own name or with a wrong name.

x. I will be responsible for my behaviour when I use the internet/learning platform. This includes resources I look at and the words I use.

xi. I will be polite and understand that other people might not think the same as me. I must respect their ideas and not be rude or disrespectful.

xii. I will not give out any personal information such as name, telephone number or address through email. I will not use the school IT to publish my personal ideas. I will not arrange to meet anyone unless this is part of a school project approved by my teacher.

xiii. I will not look at, download, upload or send on to anyone else material that could be offensive or against the law. If I accidentally come across any such things I will report it immediately to a teacher.

xiv. I will not download or install software on the school network.

xv. I will not try to get round the school internet safety wall.

xvi. I will make sure that my online activity, in school and outside school, will not cause my school, the staff, students or others to be upset or that it will not look bad for the school.

xvii. I will always respect that other people own their own work online and I will treat this as private to them.

xviii. I understand the school can check how I use the school's computer systems including websites I look at, e-mails I write and it might delete inappropriate work by me.

xix. I know that all my use of the internet and school's systems and other related technologies might be checked and staff told about what I do.

xx. I understand that these rules keep me safe and that if they are not followed, there will be sanctions and my parent/carer may be contacted. I understand that breaking the rules may result in the loss of my network or internet access.

Student name ……………………………………..…………………………………………………

I agree to follow the Acceptable Use Policy and have understood and agree with the content of the Safe Use of Technology Policy.

Student Signature ……………………………………………………………………………………….

House ………………………………… Date……………………………………….

Appendix IV.

Acceptable Use of IT Policy – Parent / Carer Declaration

All students use computer facilities, including internet access, as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign declarations to show that they agree to follow this Acceptable Use Policy and have understood and agree with the content of the Safe Use of Technology Policy.

Parent / Carer name: ……………………………………………………………

Student name: ………..……………………………………………………………

i. As the parent or legal guardian of the above student, I have read and understood the published school Safe use of Technology Policy and grant permission for my child to have access to use the internet, school email system, learning platform and other IT facilities at school.
ii. I am aware that my child has signed the Acceptable Use of IT Policy and that they have a copy of the school online-safety rules in their diary. We have discussed this document and my child agrees to follow the online-safety rules and to support the safe and responsible use of IT at Gordon's School.
iii. I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep students safe and to prevent students from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching online-safety skills to students.
iv. I understand that the school can check my child's computer files and the internet sites that they visit, and that if they have concerns about their online-safety or e-behaviour they will contact me.
v. I understand the school is not liable for any damages arising from my child's use of the internet facilities.
vi. I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's online-safety.

Parent/Guardian signature:

………………………………………………………..Date……………………………………………

Please complete, sign and return to the School Office