Grace Academy

Digital & E-Safety Policy

Policy Reference:	GA-P113
Version:	V13
Status	Operational
Authors	J. Wood
Applicable to:	Staff, Students & Parents
Checked by	IT Managers & J. Clarke
Valid From	June 2018
Review Date	June 2021

Contents

DIGITAL POLICY AND PROCEDURES

1.1 Introduction

Information Communication Technology (ICT) includes both the fixed and mobile internet; technologies provided by the Academy and technologies owned by students and staff, but brought onto Academy premises. Given the ever changing world of technology it should be noted that this applies to all forms of technology used. Including CLOUD based services.

The Grace Academy Digital policy will operate in conjunction with other policies. If you are unable to access the policies on the Portal please request a hard copy from the Principal.

Although the policy addresses specific areas of Digital, E-Safety and Social Media, all teachers have a general responsibility under the Teachers Standards to follow, both professionally, personally, within and outside of the Academy within part 2, and any other applicable part of the Teachers Standards. Support staff should follow the spirit of Grace Academy policies and demonstrate due care and attentions to their professional and personal conduct both within and outside of the Academy.

The Principal of the Academy or a Director has authority to delegate on specific role as required. There may be specific guidelines for each academy that vary slightly. i.e.: Use of mobile phones during the school day.

The data protection policy should be read in conjunction with this policy.

1.2 Definition of User

This Policy applies to any individual or organisation that works directly with the Academies; staff who breach this policy will be subject to the disciplinary policy.

This list includes, but is not exhaustive:-

- Teaching staff
- Leadership
- Non- teaching and cover staff
- Post 16 students
- Key stage 3&4 students
- Parents and carers
- Governors
- Third party suppliers
- Volunteers

1.3 Legislation

- Human Rights Act 1998
- Data Protection Act 1998 and General Data Protection Regulations
- Freedom of Information Act 2000

- Computer Misuse Act 2000, amended by the Policy and Justice Act 2006
- Regulation of Investigatory Powers Act 2000 (RIPA)

2.1 Teaching and Learning

2.1.1 The importance of the Internet and digital communications

The Internet is an essential and everyday element in 21st century life for education, business and social interaction. The Academy has an obligation to provide students with internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students to enrich learning activities.

2.1.2 Internet use to enhance and extend learning

The Academy internet access will be filtered appropriately to the age of students and the learning tasks they are engaged in. Clear boundaries will be set for the appropriate use of the internet and digital communications during learning activities and discussed with students as a pre-cursor to the learning experiences. Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation, throughout all curriculum areas.

2.1.3 Students will be taught how to evaluate Internet content

The Academy will ensure that the use of internet derived materials used by staff and students complies with copyright law and is not plagiarised. Online plagiarism programmes will be used to sample and moderate work. Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy throughout the curriculum. Students will be taught across the curriculum to acknowledge the source of information and to respect copyright when using internet material in their own work.

2.1.4 Staff will constantly monitor student activity during lessons.

2.2 Managing Internet Access

2.2.1 Information system security

The CEO in conjunction with the Principals will have the opportunity to review the Grace Academy ICT system security annually. If absent from the Academy for a period of 5 days or more your web based access may be disabled. Should there be any cause for concern the Principal may at their discretion instruct the Senior ICT Technician to suspend your access.

Web filtering or appropriate filtering systems are installed and checked regularly by IT staff. Any issues of concern are raised with a member of the senior leadership team who will deal with the matter appropriately in line with Academy policies.

2.2.2 E-mail

Staff and students may only use approved e-mail accounts on the Academy system. Grace Academy employs full SPAM and inappropriate word filtering and where necessary can monitor any incoming or outgoing emails.

Staff and students have an obligation to inform their line manager or teacher if they receive an e-mail or other digital communication that they feel is inappropriate or if they feel uncomfortable with the message content or tone. Action will be taken in accordance with the Anti-Bullying policy.

In e-mail or other digital communication, staff and students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. E-mail from staff and students to external bodies is presented and controlled in the same way as a letter when written on Academy headed paper. Therefore please ensure that any communication in this format accurately represents the views of the Academy. The forwarding of chain letters is not permitted.

2.2.3 Publishing personal contact information

Staff or student personal contact information will not generally be published externally. The contact details given online should only be the Academy administration office. The Principal or nominee will take overall editorial responsibility and ensure that published content is accurate, appropriate and current.

2.2.4 Publishing images and work

Photographs that include staff and students will be selected carefully. Students' full names will not be used anywhere on the Academy website or other public facing websites, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of students are published on any public facing website. Work can only be published with the permission of the student and parents/carers. Further details can be found in the data protection policy and consent forms will be required to be completed in full - see Annex A.

Permission will obtained from staff in respect of publication of their photographs and original work on any public facing websites.

2.2.5 Social networking and personal publishing

Staff should not access inappropriate or non-educational/non-professional discussion forums. Staff should be aware that they are responsible or accountable for any information or data they provide for publication in any format.

Staff should not access the following sites during core working hours unless by express permission from the Principal or Trust Director or as set out within as set out within their job description:

i) Social networking sites e.g. Facebook/Twitter/Instagram/snapshot
ii) Newsgroups

Social networking sites and newsgroups will be blocked unless a specific use is approved. The dangers of these websites will be taught and communicated to students through curriculum tutor activities and assemblies on e-safety and in various other applicable age related events or forums.

Staff and students will be instructed not to place personal photos on any social network space without considering how the photo could be used now or in the future. Staff and students will be instructed on E Safety security and encouraged to set strong passwords, to deny access to unknown individuals and to block unwanted communications. Staff and students should only invite known friends and deny access to others.

Staff and students should not create social networking accounts using the Grace Academy name without prior authorisation from the Principal or Directors, including the CEO.

2.2.6 Managing filtering

The Academy will work in partnership with service providers and CEOP to ensure that systems to protect students are reviewed and improved both annually and when emerging technologies dictate.

Staff will have unfiltered access where appropriate to their role. Students will have filtered access as deemed appropriate by the Principal or the CEO.

2.2.7 Managing emerging technologies

Appropriately planned pilot programmes will be carried out for emerging technologies that may be of educational or administrative benefit. These programmes will be evaluated against student engagement, positive impact on learning and/or increased productivity before they are introduced across the Academies.

2.2.8 Protecting personal data

Personal data will be recorded, stored, processed, transferred and made available according to the current UK legal guidelines and particular regard will be given to the General Data Protection Regulations (GDPR).

2.3 Policy Decisions

2.3.1 Authorising internet access

All staff and students must have read, accepted, signed and agreed to comply with the Acceptable Use Statement. Failure to sign will mean authorisation will not be granted. Digital acceptance may also be requested before use.

Unauthorised personal use of the internet within specified working hours may constitute gross misconduct and is not allowed.

Internet access for personal use may take place within the following parameters:-

a) It does not take priority over core working practices, for example, but not limited to:

i) teaching;
ii) supervising students;
iii) completing work required to meet a specified deadline.

b) It is only outside of core working hours, for example, although not limited to:
i) prior to the start of the working day as defined in your contract;
ii) at the end of the working day as defined in your contract;
iii) during a lunchtime break.

c) Any sites viewed should not contravene this policy or cause any harm to Grace Academy.

d) Copyright law should be adhered to at all times. Any information published on the internet will normally be protected by copyright. The use of software downloaded from the internet is covered by copyright rights. Unauthorised copying is a criminal offence and will be referred to the appropriate authority to action.

2.3.2 Assessing risks

The Academy will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Academy network. The Academy cannot accept liability for any material accessed, or any consequences of internet access. The Academy will audit ICT use to establish if the digital policy is adequate and that the implementation of the policy is appropriate and effective. This audit will form part of the policy review.

2.3.3 Handling e-safety concerns

Complaints of internet misuse will be dealt with by the Academy consequences systems. Any complaint about staff misuse must be referred to the Principal. Issues relating to child protection must be dealt with in accordance with Academy child protection procedures.

2.3.4 Community use of the internet

Any individuals and/or organisations that work directly with the Academies will be subject to the Responsible Use Statement and this policy.

2.3.5 Mobile devices

Personal mobile technology devices may be brought into the Academy, however each academy will make the decision as to when they may be used on academy premises.

Mobile technology devices should be switched off (unless sanctioned for professional use) and out of sight at any time inside the buildings. This includes when students are walking between lessons and at break and lunch times. Certain areas may be designated during the day.

Mobile technology may be taken out and used in lessons ***only*** with the permission of the classroom teacher and where the use of these devices has been matched to clear learning objectives in line with Local Authority procedures.

The use of mobile phones to intimidate is unacceptable and constitutes a form of bullying and will be dealt with in accordance with the relevant bullying policy for non-staff and the disciplinary policy for staff.

The Academy accepts no responsibility for replacing lost, stolen or damaged mobile technology.

Mobile devices may be permitted on Academy trips but only at the discretion of the trip leader.

The Academy does not accept any responsibility for the impact that the use of such devices could subsequently have on health and wellbeing.

2.4 Communicating e-Safety

2.4.1 Introducing the e-safety policy to students

Students will be informed that network and Internet use will be monitored. A programme of training in e-Safety will be developed in each Academy with regard to the Safeguarding Policy.

2.4.2 Digital policy

You will be expected to adhere to this policy. Network and internet traffic is monitored and can be traced to the individual user. It should be understood that phone, photographic or online communications with students could occasionally lead to misunderstandings or even malicious accusations. Therefore care must always be taken to maintain a professional relationship.

2.4.3 Enlisting parents' and carers' support

Parents' and carers' attention will be drawn to the Academy Digital and E-Safety Policy.

3.1 Bring Your Own Device: (BYOD) Acceptable Use

3.1.1 Devices

This device list applies, but is not limited to, all devices that fit the following classifications:

- Laptop/notebook computers
- Any personally-owned device capable of connecting to a guest wireless network

The policy applies to any hardware and related software that is not owned or supplied, but could be used to access Grace Academy resources. That is, devices that staff and students have acquired for personal use but also wish to use in the Academy environment. The overriding goal of this policy is to protect the integrity of the data that resides within the Grace Academy technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a device

(such as a USB memory stick) or carried over an insecure network where it could potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications and damage to the organisation's public image. Therefore, all users employing a personally owned device must only connect via the Grace Mobile Wireless Network. Wireless is WPA encrypted and requires a certificate.

Non-sanctioned use of personal devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

3.1.2 Applicability

This policy applies to all Grace Academy employees, including full and part-time staff, students, contractors, consultants, and other agents who use a personally owned device to access Academy data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Grace Academy has built with its constituents. Consequently, employment and/or attendance at Grace Academy will not automatically guarantee the initial or ongoing ability to use these devices to gain access to the Grace Academy networks and information. Each Grace Academy will decide if BYOD are allowed on the academy network due to the need to police encryption and network safety effectively.

3.1.3 Responsibilities

The CEO of Grace Academy has the overall responsibility for the confidentiality, integrity, and availability of corporate data.

Other IT, IS, and ICT staff under the direction of the CEO in conjunction with the Principal are responsible for following the procedures and policies within information technology and information systems.

All Grace Academy students and staff are responsible to act in accordance with the organisation's policies and procedures.

3.1.4 Affected technology

Connectivity of all student and staff-owned devices will be monitored by the Grace Academy IT department and will use multi-factor authentication and strong encryption measures to isolate and protect any corporate data accessed by the device where appropriate. IT will not directly manage personal devices if allowed in the academy and end users are expected to secure their own devices using a pattern, pin or password security measure. Failure to do so will result in immediate suspension of all network access privileges so as to protect the organisation's infrastructure. The academy Principal with the assistance of IT may request at any time to view the security encryptions of devices containing personal data belonging to the academy or another student or staff member. Grace Academy Solihull permit access through validated IP for staff and validated authentication for students.

3.1.5 Appropriate use

It is imperative that any mobile device that is used in Grace Academy and for Grace Academy business that is connected to the ICT network for educational purposes should

be used appropriately, responsibly and ethically and with due regard to the Responsible Use Statement. Failure to do so will result in immediate suspension of that user's account. Based on this requirement, the following rules must be observed:

3.1.6 Access control

1. The CEO, Principal or nominated person reserves the right to refuse, by physical and non-physical means, the ability to connect personal devices to corporate and corporate-connected infrastructure. The CEO or Principal will engage in such action if such equipment is being used in a way that puts the Academy systems, data, users, and students at risk.
2. Prior to initial use on the network or related infrastructure, all devices must be approved by the Principal.

3.1.7 Security

1. All users of personally owned devices must employ reasonable physical security measures; this must include a strong password, pattern or pin protection.
2. Any non-business computers used to synchronise with these devices will have installed up-to-date anti-virus and anti-malware software deemed necessary by the Grace Academy IT department.
3. Passwords and other confidential data as defined by the Grace Academy IT department are not to be stored unencrypted on mobile devices.
4. ICT will manage security policies, network, application and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Grace Academy's overarching security policy.
5. ICT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the network.
6. It is a user's responsibility to remove all organisation specific data.
7. In the event of a lost or stolen device, it is incumbent on the user to report the incident to ICT immediately. ICT will attempt to remotely wipe the device of all data to prevent unauthorised access. If the device is recovered, it can be reconfigured following the relevant help page on the Portal. The remote wipe will destroy all data on the device, whether it is related to organisation business or personal. Grace Academy does not accept any liability in respect of personal data lost through this process. This is in accordance with the Grace Academy BYOD policy.
8. Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the Academy.
9. Wireless is WPA encrypted and requires a certificate.
10. Grace Academy will not be held liable for any loss, damage or theft of your device.

3.1.8 Help and support

Students and Staff who opt in to the BYOD program are not eligible for support for device-specific hardware or software from the Grace Academy IT department.

3.1.9 Organisational protocol

1. The end user agrees to and accepts that his or her access and/or connection to the Grace Academy networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.
2. The end user agrees to immediately report to his/her manager and the IT department any incident or suspected incidents of unauthorised data access, data loss, and/or disclosure of organisation resources, databases, networks, etc.
3. While a personally owned device user will not be granted access to corporate resources without accepting the terms and conditions of this policy, staff and students are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents. By signing this policy, employees acknowledge that they fully understand the risks and responsibilities of the BYOD program.

4.1 Mobile Devices

Mobile devices are powerful communication tools. They have the ability to not only enable voice-to-voice conversations, but they also allow us to communicate via text messaging, email, and on many devices via the web. The following rules have been created to support teachers that choose to empower students to use their devices for educational purposes.

4.1.1 Rules governing the use of mobile devices

1. The use of mobile devices must have an educational objective. The use should empower you and your students to meet learning objectives that cannot otherwise be met.
2. Ensure that parents/carers are kept informed of their child's use of mobile devices in your lessons.
3. Teachers must ensure that student and parents/carers have signed the 'Bring your own device: Student Permission' document.
4. When using mobile devices to access the internet, students are required to connect using the Grace Academy Guest Wi-Fi where they will be required to go through web filtering.
5. Mobile devices should be on silent mode with vibrate-only on.
6. Mobile devices must to be in pockets or backpacks until it is time to use them.
7. Any activity conducted on mobile devices in class cannot be published without permission of the teacher and/or students who are involved in the text/image/video/audio file.
8. Students will use appropriate mobile device etiquette by respecting the privacy of other's device numbers and using appropriate language with their mobile communication.

5.1 Social Networks (Including Virtual Worlds)

5.1.1 Background

Professional standards dictate that an adult should never be alone with a student in an isolated space (e.g. one student, one teacher together in a classroom with the door

closed). This is true in online environments as well. Social networking sites are structured to be closed environments, and as such Grace Academy discourages students and teachers from using them to communicate with one another. Grace Academy provides websites, blogs, and email for students and teachers to communicate and collaborate. If a student or teacher desires to use a social networking site to communicate and collaborate, Grace Academy recommends using the Grace designated software to create a class social networking site. In such an environment the students and teachers are both protected by the monitoring and oversight of Grace Academy. The same will apply to vlogging, YouTube and other forms of live film.

5.1.2 Rules for the use of social networking

1. Teachers that feel that "mainstream sites" such as Facebook will add educational value that cannot be attained without such sites, should communicate their intentions with the Principal and before requesting site access via the IT helpdesk. Teachers must remember that they should not assume that all students have access to the internet or to social networking sites, and should not use these as the sole source of communication.
2. Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests.
3. Do not initiate friendships with students. Remember that people classified as “friends” have the ability to download and share your information with others. Post only what you want the world to see. Imagine your students, their parents, or your administrator visiting your site. On a social networking site, once you post something it may be available, even after it is removed from the site.
4. Do not discuss students or colleagues or publicly criticise Academy policies or personnel. Visit your profile’s security and privacy settings. At a minimum, educators should have all privacy settings set to “only friends”. “Friends of friends” and “Networks and Friends” open your content to a large group of unknown people. Your privacy and that of your family may be a risk.
5. Let your administrator, fellow teachers and parents know about your educational network.
6. When available, use Academy supported networking tools.
7. Do not say or do anything that you would not say or do as a teacher in the classroom. (Remember that all online communications are stored and can be monitored).
8. Have a clear statement of purpose and outcomes for the use of the networking tool.
9. Do not post images that include students without parental consent.
10. Pay close attention to the site's security settings and allow only approved participants access to the site.
11. Do not use commentary deemed to be defamatory, obscene, proprietary, or libellous. Exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions and derogatory remarks or characterisations. It is unlawful to write about a person online that exposes that person to:
    - hatred, ridicule or contempt;
    - causes his/her standing to be shunned or avoided;
    - lowers his/her standing in the estimation of right thinking members of society;
    - disparages him/her in his/her business, trade or profession.
12. Weigh whether a particular posting puts your effectiveness as a teacher at risk.

13. Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these sites are calendar programs and games.
14. Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
15. Be careful not to fall for phishing scams that arrive via email or on your wall, providing a link for you to click, leading to a fake login page.
16. If a staff member learns of information on the social networking site that falls under the mandatory reporting guidelines they must report it as required by law.
17. Republishing images or content on social media services can breach copyright law (see 2.3.1).

6.1 Blogging/Video

Blogging sites, such as Twitter, Plurk, Tumblr, etc. are excellent resources for educators to use to communicate with students and parents. In many cases, users can elect to "follow" a user and have that user's posts be sent to a mobile device or email address. In the case of the popular site Twitter, a teacher can create an account and "tweet" daily updates such as assignments, due dates, and reminders. A student or parent can follow the teacher and receive these updates on their mobile phone.

6.1.1 Rules for the use of Blogging/Video

1. Let your administrator, fellow teachers and parents know about your blogging account/site.
2. Link your blogging account with your Grace email. Any direct messaging will then be sent to your Grace email and can monitored and stored for your protection and the protection of the student/parent.
3. Post only what you want the world to see.
4. Do not discuss students or colleagues or publicly criticise Academy policies or personnel.
5. Do not say or do anything that you would not say or do as a teacher in the classroom. (Remember that all online communications are stored and can be monitored).
6. Have a clear statement of purpose and outcomes for the use of the networking tool.
7. Do not post images that include students without parental consent.
8. Do not use the micro blogging site as your sole source of communication. Messages that you send via a micro blogging site should also appear on your teacher webpage.

7.1 Parental Responsibility

7.1.1 Parents are not expected to post pictures of students other than their own children on social networking sites.

7.1.2 Parents should make complaints through official Academy channels rather than posting them on social networking sites.

7.1.3 Parents should not post malicious or fictitious comments on social media about any member of the Academy community.

A. CONSENT FORM

Child's name: _____

Date: _____

Dear Parent/Carer

At Grace Academy we take photographs of students to support student identification and safeguarding. We also take photographs at various events throughout the year and use these in the Academies prospectus, on the Academy website and on display boards around the Academy. We also use photographs in newsletters distributed throughout the local area, in press releases when celebrating student's achievements and on our Facebook and other social media platforms.

We would like your consent to take photos of your child and use them in the ways described above. If you are not happy for us to do this, that is not a problem – we will accommodate your preferences. Please note that photographs used specifically to support student identification and safeguarding must be taken.

Please tick the relevant box(es) below and return this form to the Academy.

I give consent to all of the statements below ☐

If you do not give consent for all of the statements below, please indicate by ticking the box that you give consent for.

I am happy for photos of my child to be used on the Academy website.	
I am happy for photos of my child to be used in the Academy prospectus.	
I am happy for photos of my child to be used in internal displays.	
I am happy for photos of my child to be used in the Academy newsletter.	
I am happy for photos of my child to be used in press releases.	
I am happy for photos of my child to be used on Grace Academy social media sites.	

I DO NOT give consent to any of the above ☐

If you change your mind at any time, you can let us know by emailing or calling the Academy or come into the Academy office.

If you have any other questions, please do not hesitate to contact us.

Parent/Carer name: _____

Parent/Carer signature: _____

Date: _____

B. E SAFETY RESOURCES

Below you will find a selection of e Safety resources that you may find helpful for parents and children:

- *Childnet*
- *Safe use of new technologies in School (OFSTED 2010)*
- *Keeping Safe*
- *Child Exploitation and Online Protection Centre*
- *Resources for Parents*

C. ACCEPTABLE USE POLICY

ICT Acceptable Use Policy

ICT members of staff should request an ICT acceptable use policy specific to their role to sign.

The ICT systems at Grace Academy must always be used by staff/students/parents/governors and contractors/guests in an appropriate manner. The Academy reserves the right to monitor any ICT usage and examine or delete any files that may be held on its ICT system. In the event of misuse the relevant Principal/Director will determine the appropriate sanction.

Rules for responsible computer use

The Academy has installed computers and also offers access to the internet, Academy email, and the Academy portal to aid access to information onsite and offsite. Like all Academy equipment the ICT computers and network resources should be treated with respect. In using the Academy ICT equipment you must agree to the following terms:-

- I will only access the system with my own usernames and passwords, which I will keep a secret and not share with fellow students or colleagues.
- I will not access, or attempt to access, other users' files.
- I will log off correctly and leave all equipment in the same state as I found it.
- I will not cause damage to or interfere with any of the ICT equipment.
- I will report any damage and not attempt to repair, replace, or swap, any faulty ICT equipment.
- I will not display, print or distribute, in any form whatsoever, material that may be regarded as offensive (promoting discrimination of any kind) or copyrighted.
- I will not try to access pornographic, racist or offensive material.
- I will not enter public or private chat rooms.
- I will only email people I know, or that a member of staff has approved.
- I will not open email attachments from an untrustworthy or suspicious source.
- I will not send anonymous messages or forward chain letters and I will not send messages which appear to come from someone else.
- I will not give my home address or telephone number, or arrange to meet someone, unless an appropriate Academy staff member agrees and my parent or carer has given permission. I will be aware of 'stranger danger' when online.
- I will report any unpleasant material or messages sent to me immediately.
- I will not compromise the security of ICT systems, whether owned by the Academy or by other organisations or individuals (including attempting to bypass internet security filters).
- I will not use my own software, or attempt to install any new software, on any Academy computers.

- I understand that copyright and intellectual property rights must be respected. I will not use the Academy ICT systems to plagiarise.
- I understand that the Academy may monitor my computer usage, including any saved files, internet sites I visit, and the contents of my email messages.
- I will not copy or download music, pictures or video files to the Academy network for personal use.
- I will not listen to online music or watch online videos without an appropriate Academy staff member's permission.
- I will not take photographs or record videos of anyone without their permission.
- I will not use the Academy ICT systems for online gaming, online gambling, file sharing, or financial gain unless approved by the Principal in writing.
- As a staff member I will pay particular attention to the limited use of social sites and personal internet use during core working hours as defined in section 2.2.5 and 2.3.1. and confirm that I have read and agree to adhere to the data protection policy.

Signed: ……

Name (please print): ……

Date: ……

Parent/Guardian Signature (if required)

Signed: ……

Name (please print): ……

Date: ……

D. BRING YOUR OWN DEVICE, STUDENT/STAFF PERMISSION

You are allowed to bring your own device into the Academy, if you follow these rules and procedures:

1. You can only connect to the Grace Wireless System.
2. You must first seek permission for the use of your device by getting your parents/carers to sign this summary.
3. You will be expected to have a strong password, pin or pattern password to protect your device.
4. You must also ensure that you have taken reasonable precautions to stop viruses entering the Grace Academy Network by installing the latest virus protection software.
5. If your device is lost or stolen you must inform ICT immediately and we will have the right to wipe the device of all data to prevent unauthorised access.
6. Grace Academy can offer no technical support for your device.
7. Grace Academy will monitor your access to our network.
8. Grace Academy will not be held liable for any loss, damage or theft of your device.
9. Grace Academy withhold the right to block any website/service.

Student and Parent/Carer Declaration

I/We, , have read the Digital Policy and consent to follow the rules and guidelines.

_____ _____
Student signature & printed name Date

_____ _____
Parent/Carer signature (if required) Date

_____ _____
Staff signature & printed name Date