St. Mary's C.E. (A) Primary School

Greenfield

Acceptable Use Policy

Last reviewed Autumn 2022

Next review: As appropriate in relation to any changes in legislation or policy.
This policy will stand until the next review.

ST MARY'S' C.E. (A) PRIMARY SCHOOL GREENFIELD

CURRENT ACCEPTABLE USE POLICY

MISSION STATEMENT

'We enjoy learning and achieving in a Christian environment'.

Having gifts that differ according to the grace given to us, let us use them: if prophecy, in proportion to our faith.

Romans 1:20

Equality Statement

This policy and procedure is subject to The Equality Act 2010 which recognises the following categories of individual as Protected Characteristics: Age, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual orientation and Disability.

KCSIE

This policy and procedure is subject to the statutory safeguarding and child protection guidance for schools in England, Keeping Children Safe in Education (KCSIE, DFE 2022) which outlines a child-centered and coordinated approach to safeguarding. Safeguarding and promoting the welfare of children is everyone's responsibility and every person who comes into contact with children in whatever capacity has a role to play. They should therefore consider, at all times, what is in the best interests of the child and take prompt action where necessary.

Data Protection Statement

The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.

All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What ?	**Probable Content**	**Why ?**	**Who ?**	**Where ?**	**When ?**
None	n/a	n/a	n/a	n/a	n/a

As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	**Has A Moderate Level of Data Compliance Requirements**	**Has a High Level Of Data Compliance Requirements**
✓		

Introduction

At St Mary's Primary School we understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy includes the use of fixed and mobile internet technologies provided by the school (such as PCs, laptops, iPads, interactive whiteboards, digital video equipment, etc.)

The computer system is owned by the school. 'The computer system' means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken offsite.

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will, however, endeavour to add any important issues to the policy on our website.

Why do we need an acceptable use policy?

Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences, or allow adults to enhance their own professional development. ICT or computing is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people, and adults. The school recognises the need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment and also the control of their use to ensure the protection and safety of all.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Twitter
- Facebook
- Snapchat
- Whats App etc.
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

- Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

The installation of software or hardware unauthorised by the school, whether legitimately licensed or not is **expressly forbidden.**

The school reserves the right to examine or delete any files that may be held on its computer systems or to monitor any internet sites visited.

All members of staff, students on placement, supply teachers etc must sign a copy of this policy statement before using the systems of the school. All children must be made aware through class discussion of all the important issues relating to acceptable use.

How does Internet use enhance our school environment?

The purpose of Internet access in schools is to raise educational standards, support the professional work of staff and enhance the school's management, information, and business administration systems.

Teachers and pupils will have access to websites worldwide (including museums and art galleries) offering educational resources, news, and current events.

Appropriate and relevant arrangements will be made where necessary for Continuing Professional Development and Training. This may take the form of commissioned support from quality-assured consultants, collaborative support from the Dovestone Learning Partnership, peer-to-peer support etc

Parents' and carers' attention will be drawn to our ICT policies in our school brochure and on the school's website.

Internet/Computing Access Policy Statement

In common with other media such as magazines, books, and videos, some material available on the Internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter upsetting, offensive, or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person;
- The internet may be accessed by staff and children throughout their hours in school;
- Our internet access has a filtering system that prevents access to material inappropriate for children;
- Children using the internet will be working in the classrooms and will be under the supervision of an adult at all times.
- Staff will use their professional judgement and check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils;
- Our rules for Responsible Internet Use are posted near all computers with Internet access.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LEA, our Internet Service Provider, and the DfEE.
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited;
- Users are responsible for all e-mails sent and for contacts made that may result in an e-mail being received. Due regard should be paid to content. The same professional levels of language should be applied to letters and other media;
- Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded;
- Copyright of materials must be respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon may be in breach of the General Data Protection Regulations, Individual Copyright, or Intellectual Property Rights;
- Use of materials stored on the school's network for personal financial gain is excluded;
- Posting anonymous messages and forwarding chain letters is excluded;
- The use of the internet, e-mail, or any other media to access inappropriate materials such as pornography, racism, or any other offensive material is forbidden;
- Children must not be given unsupervised access to the internet. For the purposes of this policy, 'supervised' means that the user is within direct sight of a responsible adult;
- All teachers within all year groups should be including internet safety issues as part of their discussions on the responsible use of the school's computer systems;
- All children must be taught to understand that if they see an unacceptable image on a computer screen, they must turn the screen off and report immediately to a member of staff.
- Breaches of the Acceptable Use Policy by pupils or use of inappropriate language on computing applications will be dealt with in a variety of ways, including removal of internet access rights, computer system access rights, meetings with parents, or even exclusion; in accordance with the severity of the offence and the school's Behaviour policy.

Evaluating Internet Content

Children will be introduced to the St Mary's Rules of Responsible Internet Use from Y2 upwards (see appendix). A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable. If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children is taken by the class teacher, the Computing Subject Leader, and the Senior Leadership Team. Awareness of the safe use of the internet will also come through Safer Internet Week which occurs in February each year.

Email Management

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between neighbouring villages and other schools.

The government has announced that whole-class or group e-mail addresses should generally be used in primary schools – this is the approach which we will use at our school if necessary- thus limiting the dangers.

The LA monitors and filters all staff emails on First class. First Class is to be used for emailing other people who work in education within Oldham – it is not to be used for social email – i.e. for emailing friends from other organisations. Staff are permitted to use both a personal account i.e. a Hotmail/AOL account at school providing they follow the school's policy on acceptable use. E-mail sent to an external organisation i.e. newspaper should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be.

Website Management

Our school website celebrates pupils' work, promotes the school as well as having class information and home learning. Editorial guidance from ICT personnel will ensure that the Web site reflects the school's ethos that information is accurate and well presented and that personal security is not compromised. Although there are many ways to obtain information about schools and pupils, for instance, a school newsletter, a school's Web site can be accessed by anyone on the Internet. Publication of the information should be considered from a security viewpoint. To ensure the safety of all our staff and children we will ensure pictures included on the website will be relatively small photographs of groups of pupils and wherever possible using photographs that do not show any faces at all. "Over the shoulder" can replace "passport-style" photographs but still convey the educational value of the activity.

Under GDPR regulations, all parents and carers are required to complete a consent form for use of photographs in school; this includes on the school website.

The point of contact on our school Web site will be the school address, school e-mail, and telephone number. Staff or pupils' home information will not be published. The Headteacher and Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Emerging Internet Applications

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as iPad's, PDAs, gaming devices, mobile, and Smartphones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

At St Mary's we will ensure that we stay up to date with new technologies wherever possible, including those relating to mobile phones and hand-held devices, and be ready to develop appropriate strategies. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Internet Publishing Statement

The school wishes the school's website to reflect the diversity of activities, individuals, and education that can be found at St Mary's C.E. Primary School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small the risk may be. Therefore when considering material for publication on the Internet, the following principles should be borne in mind:

- No video recording may be published without consent of the parents/legal guardian of the child concerned
- Surnames of children should not be published, especially in conjunction with photographic or video material
- No link should be made between an individual and any home address (including simply street names)
- Where the person publishing material suspects that there are child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. Please ensure before publishing any material that you refer to the GDPR consent list kept in the office.

Pupil Awareness of this Policy

All the staff, including members of the wider workforce, should share responsibility for e-safety. Assemblies, personal, social, health, and education lessons, and an age-appropriate curriculum for e-safety all help pupils to become safe and responsible users of new technologies.

As children's perceptions of the risks of internet use will vary, the rules may need explanation and discussion. Children should be reminded of the school Rules for Responsible Internet Use. Posters that state what responsible use of the internet should be up in each classroom. In addition, as part of the new ICT National Curriculum in 2014 children will be taught to;

KS1

- recognise common uses of information technology beyond school
- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

KS2

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems, and content that accomplish given goals, including collecting, analysing, evaluating, and presenting data and information
- use technology safely, respectfully, and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Staff Awareness of this Policy

The school acceptable use policy will only be effective if all staff subscribe to its values and methods. Internet safety will be included in the induction of new staff.

All staff must read and sign to show acceptance of the ICT Acceptable Use Policy for Staff before using any Internet resource in the school.

Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Breaches of the Acceptable Use policy by staff will be reported to the Headteacher and will be dealt with according to the school's disciplinary policy, or through prosecution of law.

ICT System Security Mantenance

The school ICT systems will be reviewed regularly with regard to security. Virus protection is installed on all computers in school and updated regularly. All laptops provided by the school are encrypted to ensure safety and security measures are upheld. Files held on the school's network will be regularly checked to monitor for security breaches.

Portable Equipment

The school provides portable computing equipment such as laptop computers, IPADS, and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities. The use of USB sticks and hard drives is prohibited by staff in school or external agencies.

- Equipment such as laptop computers are encouraged to be taken offsite for use by staff in accordance with the Acceptable Use statement and internet access policy and the equipment is fully insured from the movement it leaves the school premises. Note: our school insurance policy provides cover for equipment taken offsite, provided it is looked after with due care, not left in view on a car seat etc;
- Any costs generated by the user at home, such as phone bills, printer cartridges etc, are the responsibility of the user;
- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc) or maternity leave, arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to arrange to return it;
- If an individual leaves the employment of the school, any equipment must be returned;

- No software whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software. Please see permission for any software installations from the Head Teacher in the first instance.

Use of own devices in school i.e. mobile phones

- Children in Year 6 only are able to bring mobiles to school providing they have completed an appropriate consent letter
- Parents must put a letter in writing to the Head Teacher outlining the reasons why their child has need of a mobile phone
- Consent will then be given by the Head Teacher where appropriate
- The children are to give their mobile phone to the teacher on arrival in the classroom
- These will then be stored in a locked container in the office
- The mobile phones will be returned to the pupil at the end of the day
- School does not accept responsibility for the loss or damage of any mobile phones whilst on school premises;
- Staff may have mobile phones in school, but they must be turned off in lessons and all staff must not make or accept calls during times in classrooms or when working with pupils in other areas of the school.
- Staff must not use mobile phones in staff meetings;
- Mobile phones can be taken on all outside visits from the school so that contact with the school is maintained at all times;

Next review: 2025 or as appropriate in relation to any changes in legislation or policy. This policy will stand until the next review.

St Mary's C. of E. (A)Primary School
Rules for Responsible Internet Use – Pupils

Our school has computers and iPads with Internet access to help our learning. These rules will help keep us safe and help us be fair to others.

Using the Internet:

- I will ask permission from a teacher before using the internet;
- I understand that the school will not accept bullying in any form.
- I will be careful with all communications making sure that anything I write cannot be mistaken as bullying. I will not use rude or unkind words and follow out SCARF principles in communicating through the internet;
- I understand that I should report any incidents of bullying.
- I will report anything that makes me feel uncomfortable or any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number under any circumstances;
- I will only download, use or upload material when an adult at school tells me I may

Using the computers:

- I will not access other people's files;
- I will not bring in memory sticks or CD ROMS from outside school and try to use them on the school computers without my teacher's permission;
- I will not deliberately look for, save or send anyting that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately;
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my eSafety.

Remember- Always tell a teacher straight away if you are upset or worried about something that has happened online.

ICT Acceptable Use Policy for Staff

Computing and the related technologies such as email, the internet and mobile devise 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 Computing. All staff are expected to sign the policy agreement consent sheet and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head Teacher/Computing Subject Leader.

Access

As a staff member at St Mary's, I have access to the following ICT facilities:

- Computers throughout the school, Smartboards or large flat panel displays in teaching rooms.
- A secure username and password for logging into school computer systems.
- An accredited, filtered Internet connection from any computer in school or Wi-Fi connected device.
- My Documents – personal user space on the school network.
- Internal and external remote access to the school network and First Class to store and share learning resources.
- A personal @greenfieldstmary email account with email storage space.
- Access to network printers and copiers.
- Access to resources such as scanners, digital cameras, iPod touches, visualisers, iPads and microphones.
- Access to the School Management Information Systems (SIMS.net) as appropriate to role in school.

E-safety

- I will ensure that I am aware of e-safety issues affecting staff and pupils.
- I will regularly remind pupils of the Rules of Responsible Internet Use.
- I will report any accidental access to inappropriate material to the Head Teacher.
- I will be vigilant when asking students to search for images.
- If a student accesses inappropriate material I will report it following the correct procedures Head Teacher or Computing Subject Leader
- If I suspect a child protection issue I will report it following the correct procedures.
- I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

Computer Security

- I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (e.g. printers and projectors) and their cabling.
- If I notice that ICT equipment or software is damaged or not working correctly, I will report it straight away.
- I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
- I will never attempt to install software on school computers or mobile devices myself (unless I have ICT Personnel's permission).
- I will always keep my user account credentials secure and not tell them to anyone else.
- I understand that my staff logon gives me access to systems and information that students and other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials.
- I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending email whilst pretending to be another person or accessing another person's files. If I find that I do have access to an area that I know I should not have access to, I will inform ICT support personnel immediately.
- If I think someone else has obtained my logon details, I will report it to ICT support personnel as soon as possible to get my logon credentials changed.
- I will never knowingly bring a computer virus, spyware or malware into school.
- If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to ICT support personnel.
- I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network
- I will take care if I eat or drink whilst using ICT equipment.
- I will not reply to spam emails as this will result in more spam. Delete all spam emails.

- I am personally responsible for the care of ICT equipment loaned to me by school. If I lose or misplace any portable ICT equipment I will inform ICT support personnel immediately, and may have to personally replace the item.

Inappropriate Behaviour

- I will not store, download or distribute music, video or image files on my personal user space or shared area, unless they are appropriate files that I need for school.
- I will not send or post defamatory or malicious information about a person or about school.
- I will not post or send private information about another person.
- I understand that bullying, manipulation or exploitation of another person either by email, online or via text message will be treated with the highest severity.
- I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
- If I am planning any activity which might risk breaking the ICT Acceptable Use Policy (e.g. research into terrorism for a legitimate project), I will inform the ICT Personnel beforehand to gain permission.
- I will not take a photo or video of a student or another member of staff without their permission.
- I will not load photos or videos of other staff and students to websites or social networking sites. I will refer this job to ICT support personnel.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will not upload content that is inappropriate, offensive or even illegal to my online spaces at school or personal, or post material that could damage the reputations or the reputations of others, or breach intellectual property rights

Monitoring

- I understand that all Internet and email usage will be logged and this information could be made available to my manager on request.
- I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required.
- I will not assume that any email sent on the internet is secure.
- I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without the person's knowledge.

Best Practice

- I will only print out work that I need as a paper copy – where possible I will use school systems such as email and shared folders to share information electronically.
- I will report to ICT personnel/office staff if I believe a printer is not working or out of toner.
- I understand that my @greenfieldstmary e-mail is a work e-mail account, and as such will be used for professional purposes.
- I will only open attachments or download files from trusted sources.
- I will not view, download or distribute material that could be considered offensive or pornographic.
- I will obtain the school cameras (or SD cards) photograph and video trips and relevant events (I will not use my own cameras without prior arrangement).
- I will pass relevant photographs and videos taken on to the ICT Personnel for storage on the school network (I will not keep images and videos of pupils in my personal user space and will ensure they are on a shared networking area).
- I will save work regularly using sensible folder and file names
- I will organise my files in a sensible manner and tidy my user space and shared resource areas regularly.
- I will ensure that I regularly back up any work that is not saved onto the school network.
- I will seek advice from ICT support personnel before ordering any ICT equipment for my department.
- I will support and promote the school's e-Safety polocuy and help pupils to be safe and responsible in their use of Computing and related technologies

Data Protection

- I will not share any school data or protected information (including school images) with any third party organisations/other schools without seeking advice first
- I will ensure that I am aware of data protection issues and understand what is considered to be 'personal data'.
- I will not display sensitive information or 'personal data' on a public display or projected image (e.g. a smartboard). This includes student data in SIMS.net.

- I will never leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave 'personal data' unprotected.
- I will inform the Head Teacher and DPO immediately if I am involved in a data breach.
- I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.
- I will switch off my laptop when leaving the school building to ensure that it is encrypted during transit.

Social Networking / Electronic Communication

- I will not communicate with parents / students through social networking sites.
- I will ensure that any personal social networking accounts that I have are secure and private. This means nobody can view my personal content without me authorising it.
- I will never create a social networking profile, blog or account and use it for school purposes without prior written authorisation from the ICT Manager.
- I will never create a bogus social networking account or site that is associated with a member of staff, students or the school.
- If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, students or the school, I will inform the Head Teacher and ICT Personnel immediately.
- I recognise that as an organisation, we **do not use** social networking sites to communicate with students, staff and parents.

Sanctions

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of ICT equipment in school, but also applies to my use of school Trust ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include, in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the schools ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

- Signed_____

- Print Name:_____

- Reviewed 11.11.22

BRINGING YOUR OWN DEVICE POLICY

Agreement

Please read and sign the agreement below. No child will be permitted to use personal technology devices unless the agreement is signed and returned to show that you both understand and accept the terms of the agreement.The agreement is made between ..... and **Greenfield St Mary's**

Members of the school, wishing to use their personal devices on the **school** site must also adhere to its: Code of conduct, Internet Acceptable User Policy and Anti-Bullying policy. Please read carefully and initial every statement to show that you both understand and accept each one as part of this agreement:

Statements	**Initial**
1. I am fully responsible for my device(s). I understand that **Greenfield St Mary's** is not responsible for the device(s) in any way.	
2. I am not permitted to leave my personal device(s) at **Greenfield St Mary's outside** "school hours".	
3. When not in use for educational purposes my device(s) must be left "on silent" to prevent any disruption and be put away when asked to by teachers.	
4. I must immediately comply with any teacher's/classroom assistant's requests to shut down or close the screen on my device(s).	
5. I understand that I am not permitted to either transmit or upload photographic images/videos of any person on the **Greenfield St Mary's** grounds to the Internet, other than school approved sites.	
6. I am responsible for charging my personal device(s) before bringing it/them to school so it/they can run on their batteries whilst at school. Charging may not always be available and it will always be at the discretion of teachers.	
7. I understand that **Greenfield St Mary's do** not accept any responsibility for damage to my devise under any circumstances including damage caused by connecting to the school network and any infection by malware.	
8. To ensure appropriate Internet filters are in place, I understand that I can only use the **Greenfield St Mary's Wi**-Fi connection in the school site and will not attempt to bypass the network restrictions by using a 3G or 4G network.	
9. I understand that I must take all reasonable steps to avoid bringing devices onto the **Greenfield St Mary's** premises that might infect the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information. Failure to do so is in violation of the Acceptable Use Policy and will result in disciplinary action in accordance with the Schools Behaviour Policy.	
10. I accept that **Greenfield St Mary's** has the right to examine any device that is suspected of causing problems or is the source of an attack or virus infection.	
11. I accept that printing from my personal device(s) is **not permitted**	
12. I understand that I must not physically share my personal devices with other students, unless I have written parental permission to do so.	
13. I agree that my device(s) cannot be used during assessments of any kind unless otherwise specifically directed by a teacher.	

I understand that the use of personal device(s) on **Greenfield St Mary's site** is only permitted in so far as it supports my educational experience. It is not a right but a privilege, and I understand that any breach of these rules may result in the removal of this right at any time and without notice. I also understand that any breach of these rules may result other disciplinary action. I confirm that I understand and agree to follow the above rules and guidelines.

Name: Signature: Date: