ROOKS HEATH SCHOOL
Strive to be your best

ACCEPTABLE USE OF ICT POLICY

Term of policy: Every 3 years
Approved by: Board of Trustees
Date ratified: 11.02.2021
Next Review Date: Summer | 2024

Author: M Manderson

Sources: NGA, The Key
Online location:
SLICT Team/ ICT Policy
Consulted with JCC? Yes No

Introduction
This policy replaces any previous policy and follows the DfE regulations.

In line with the School's Equal Opportunities and Special Educational Needs policies, we aim to give all students equal opportunities to take part in all aspects of School life, as far as is appropriate, practicable and compatible with giving regard to health and safety and the efficient education of other students.

The policy will follow the five principles of the Children's Plan:

- to support parents and families
- to allow children to reach their full potential
- to enable children to enjoy their childhood whilst preparing for adult life
- to provide services in response to children and family needs
- to use preventative measures to help students avoid the possibility of failure

This policy is based upon the School's commitment to the development and maintenance of good behaviour and a positive and inclusive ethos for all members of the School community.

The School will ensure that the policy is applied fairly to all employees and does not have a negative impact in relation to the school's equality strands: race, sex, religion and belief, sexual orientation, age, disability, gender reassignment, marriage and civil partnership and pregnancy and maternity.

Foreword

Rooks Heath School is a mixed 11 to 18 multicultural comprehensive in the London Borough of Harrow. This policy is formulated by the Headteacher, in consultation with staff, particularly ICT & Computing staff, and is monitored by other members of the School's Leadership and Management Group. The policy is subject to review every 3 years by the School's Leadership and Management Group and is subject to approval by the governors of the School.

Due to the ongoing advancement of ICT, procedures outlined in this policy may change before the policy is due for review.**Aims of this policy**

- To ensure that the School's digital resources are used safely and in a professional manner
- To safeguard students and staff from ICT related issues and ensure that RHS community is an e-safe community

Introduction

This policy is based on government guidance on the acceptable use of ICT systems. It has been agreed by the senior management and approved by the governors. The policy will be implemented by all staff and students and will be monitored by the Network Manager and the Headteacher.

Due to the nature of the internet, social media and advancement in digital technology, it is accepted that there is no technical solution that can consistently guarantee to prevent the misuse of ICT, cyber-bullying or the access to unwanted internet material. The School will not accept liability for the material accessed or any consequences of Internet access thereof.

However, such circumstances will be carefully monitored, recorded and dealt with in accordance with this policy. The School treats e-safety as an important aspect for education and encourages parental involvement in the implementation of this policy. *Securus,* the School's monitoring system, is used to protect students and staff from the risks associated with the use of the internet and ICT systems.

Why ICT is important for students and staff

The purpose of ICT and Internet use is to raise standards, promote student achievement, to support the professional work of staff and to enhance the School's management administration systems. ICT and the internet is part of the statutory curriculum and a necessary tool for staff and students. The internet enables access to world-wide resources and access to the School's Managed Learning Environment (MLE). The School's internet access is expressly for student and staff use for educational purposes and includes appropriate filtering and monitoring (by LGfL and the School). If staff or students discover unsuitable sites, the URL (website address), content is to be reported to the ICT Support Team for these URLs to be immediately blocked.

Passwords

Access to School ICT systems may only be made with the user's authorised username and password, which must not be given to any other person. Passwords for all users will be reasonably complex and will be at least alpha numeric and subject to at least annual change.

Use of digital and video images on the website and the management of School's website and MLE

The point of contact on the website will be the School address, email and telephone number. No personal or social media information of students, staff or contractors will be published by Rooks Heath School on any website.

Parental permission is obtained for using photographs of students as part of our consent form.

The Headteacher, Director of Business and the **Assistant Headteacher with responsibility for marketing and promotion** will oversee and authorise the website's content and check the suitability of any images used. Uploading of information to the website will be restricted to staff members nominated by the **Headteacher** or the Director of Business.. Digital images of students and staff will be stored in the secure area of the School network without the written permission of the person or patent/carer. Parents are required to give consent for photographs to be used for publicity.

Staff with responsibility for managing and accessing personal data in the School's Management Information Systems or the MLE, will comply with the following conditions:

1. The data is to be used only for educational purposes or the business function of the Academy.
2. Personal data is to be shared only with those who need the information to discharge a statutory education function and will not be sent outside of the Academy without explicit approval from the **Headteacher** or the Director of Business.
3. Only authorised users may access the system and they must never share their login details with anyone.
4. Management of Canvas / Microsoft Office 365 usernames and passwords is the responsibility of the authorised system manager, under the direction of the MLE administrator in the School.
5. Any confidential or personal data will be handled with strict confidentiality and any printed material, that has personal details, will be shredded when not required.
6. Temporary data sets, mainly from SIMS or systems that hold personal information, will be deleted as soon as possible, usually on a daily basis. It is the responsibility of the user to ensure that data sets are secure and cannot be misused or misplaced. Data taken off site must be encrypted.
7. Permanent data will be deleted from all School systems and devices by individual staff members and staff in charge of data sets, such as the Network, Data and Exams Managers, who will do so in line with current GDPR regulations. In cases when there is no further need to keep such data, this will be deleted sooner. We recognise that the regulations continue to change and we will comply with these changes as soon as required.

Failure to comply with these conditions will be considered as Misconduct and potentially Gross Misconduct.

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. The School, in conjunction with LGfL, will have a default setting to block social networking sites. The restriction to use some sites may be bypassed with agreement and authorisation from the Headteacher and the Network Manager. Forums set up within the School's MLE will be acceptable.

It is the responsibility of Parent and Carers to manage and control what is published by their child at home on social media and the internet.

How will emails be managed?

Students must use the school's main communication email system to communicate with staff. Students must not use their own external personal email addresses to contact staff and staff must never respond to student personal email addresses. Students are told to immediately tell a teacher if they receive offensive email and not to reveal details of themselves or others in email communication. This includes information such as their address or telephone number. They are told not to arrange to meet anyone. Emails sent to an external organisation should be written as carefully as a letter written on School headed notepaper.

Staff will use the school's main email system within the Canvas / Microsoft Office 365 platform. The School's email disclaimer is expected to be added to emails sent to addresses external to the School.

No member of staff or student is allowed to send any personal information, relating to others, outside of the School without the explicit approval of the **Headteacher** or the Director of Business.

Mobile devices

Mobile phones (or similar mobile devices that can access the internet, record and transmit text, sound, images etc.) will not be used by students during lessons or formal School time unless expressly agreed by the class teacher for specific one-off educational purposes. The recording and sending of abusive or inappropriate text messages, sounds or images (still or moving) is forbidden and will be dealt with according to our Behaviour, Rewards and Sanctions policy. The use of recording technologies by staff is only permitted to facilitate students learning and must be done using recognised School equipment

Where School mobile phones have multiple users, the usage will be closely monitored. Users will sign for these and take full responsibility for these whilst in their care. Pin codes for mobile phones will be kept secure. At the end of the loan all data will be deleted from the mobile phone. The **Headteacher** will monitor this. Any apps downloaded for the activity will be deleted. Staff must never use their personal devices to capture images of students or internal data unless there are exceptional circumstances. Images of students (e.g. on trips) must be taken using School equipment. *See also Appendix E.*

Internet access

Students and staff must read the guidelines for acceptable use of digital devices and agree to abide by the 'Acceptable use of digital and ICT devices' policy on each occasion they use the School's ICT systems before access is given. *(See Appendix A).* Parents also sign a Consent form when their child joins the School agreeing to their use of the internet and other ICT facilities. This information is stored in SIMS and the hard copy filed with the student's records. The Network Manager is responsible for ensuring that only students who have parental consent have access to the internet.

Filtering internet access

Blocking strategies by LGfL and the School help prevent access to a list of unsuitable sites or newsgroups. The ICT Support Team will maintain and update the blocking list as new sites appear. The Network Manager will monitor internet sites visited by individual users, along with their use of our ICT systems, with the aid of *Securus*. All sites are blocked until LGfL receive a request to allow the site to be viewed. Any requests to unblock a site need to be made to the Network Manager and authorised by the Headteacher or Director of Business. Only sites that are approved will be accessible.

Dealing with Inappropriate Use of School ICT Equipment

Staff and students are expected to follow any guidance contained within this policy. Users are expected to use the systems safely and responsibly, particularly when accessing and using sensitive data. ICT support staff are expected to keep the system as safe and secure as possible by using appropriate software, such as anti-virus programs. *See also the Data Protection policy*.**Students**

Responsibility for handling student incidents is carried out by the appropriately linked Head of Year, the Headteacher or Deputy Headteacher for Pastoral care**.** The Network Manager and the Deputy Headteacher for Pastoral care, supported by Heads of Year, will monitor Securus at regular intervals. Depending on the severity of the incident, any potential misconduct will be managed in accordance with the Behaviour for Learning policy by the relevant senior aforementioned senior leader and appropriate consequences applied. An incident log together with a register of banned students is kept and monitored by the ICT Support staff, who will contact the Headteacher, Deputy Headteacher for Pastoral care or a member of the Pastoral Team including the Student Support Hub if necessary. All misdemeanours involving inappropriate use of ICT should be recorded on SIMS. See also the Behaviour for Learning policy.

Staff
Staff who use School equipment inappropriately will be dealt with using the procedures outlined in the School's HR policy. It will be deemed Misconduct or Gross Misconduct, depending on the level of failure or degree of abuse. Responsibility for dealing with staff misuse will sit with the Headteacher, or the Deputy Headteacher in her absence. A record of any staff who have misused ICT inappropriately is kept by the Headteacher. See also the HR policy.

Governors
Governors and Trustee members have limited access to the ICT systems and have access to approved and secure areas of the School's MLE (Canvas / Microsoft Office 365). Governors have a duty to uphold this policy in the same way as the staff.

Regulation of chat rooms, newsgroups, forums and RSS feeds
Students will only be allowed access to approved chat rooms, newsgroups, forums and RSS feeds with the approval of the Headteacher in consultation with the Network Manager.

Security of the ICT system
The School's ICT Support Team will be responsible for installation and regular updating of virus protection. Use of personal portable storage media such as USB memory sticks, DVDs, CD-ROMs and other portable storage devices are reviewed on an as and when basis. *See also below.* Access to files are automatically scanned in 'real time' and reports are sent to ICT Support. *See also the Rooks Heath Critical Incident* and *Data Protection policies.*

Portable devices
Personal portable devices cannot be connected to the School system. However, exceptions are made for certain subject areas, such as Photography or Media where files are very large and for certain cases at the discretion of the **Headteacher** in consultation with the Network Manager. Mobile phones which belong to the School will have access to the School's wifi signal. A select group of students studying vocational courses have access to laptops which are managed on the School's network when on site.

Software
Only software approved by the School will be installed on School computers and only ICT support staff have the necessary permissions to do this. Unlicensed and Open Source software (for example Audacity and Scratch) cannot be used on the School's system unless these are authorised and cleared by ICT Support and the Headteacher or Director of Business. Only the Network Manager can authorise software installation of software by the ICT support team.

Backups
The Network manager is responsible for encrypted backups of all School systems which are made and kept off site, currently using Gridstore.

Loss of ICT Equipment
In the event of complete loss of the School's ICT equipment, the ICT Support Team will be responsible for getting the systems working again. Cloud based services will also cause downtime if these services fail. This is likely to take at least 6 weeks. The costs at the time of writing this policy are indicated below:

Item	**Quantity in school**	**Cost per item**	**Total Cost**	**Life cycle in years**	**Notes**
Computers	537	£220 - £450	£118,140 - £241,650	5	*£220 being on the refurbished spectrum with the higher price being for new models*
Projectors	68	£600	£40,800	3	
Laptops	144	£229 - £400	£32,926 - £57,600	5	*60 are student / DFE assignments 64 are staff laptops.*
IWB	68	£1,500	£102,000	5	
AIO IWB	2	£2,500	£5,000	5	
Colour Printers	35	£200-300	£7000-£10,500	5	
BW Printers	30	£150-200	£4,500 - £6,000	5	
Speakers	71	£100	£7,100	5	
Servers	5	£3,000	£15,000	3	
SAN	1	£10,000	£10,000	5	*SAN price factored alongside disk requirement*
UPS	2	£1,500	£3,000	3	
Switches	38	£800 - £1,500	£30,400 - £57,000	6	*POE factored 24 port and 48 ports more expensive than previous outline as the switches specs were very primitive and not sufficient*
Wireless Point	50	£200 - £300	£10,000 - £15,000	5	
Bulbs	67	£160 - £250	£10,050 - £16,750	1	
Monitors	660	£100	£66,000	5	
Wireless Controller	1	£2500 - £3000	£2500 - £3000	5	
		Total	**£464,416 - £656,400**		

Protecting Data
Staff are able to access student data off site as long as they have a genuine need to do so and within the confines of the School's managed learning environment(s) or MIS. Currently the MLEs in use are Canvas and Microsoft 365 and the MIS is SIMS. Microsoft 365 is a highly secure environment that offers extensive multi-

layer protection. Data on Canvas will be encrypted or password protected and deleted at the earliest opportunity. Data within the 365 platform is encrypted. Once data is downloaded, this is no longer encrypted. Staff have a duty to ensure all data downloaded is protected and kept secure. This is enabled by password-protecting documents of extremely sensitive nature. Data must never be forwarded onto unauthorised users whether they are part of the School community or not. Printed data should never be taken off site unless approved by the Data Protection Officer and signed off. Failure to comply with this could be classed as gross misconduct. Any authorised data used off site will be encrypted using tools provided by the Network Manager. Where pages have been printed, these will be shredded at the earliest opportunity.

Although encryption is recommended for protecting data in the UK, some countries ban the use of encrypted data. When travelling to other countries as part of an educational visit, where encryption is not permitted, trip organisers should contact the DPO or ICT Support before leaving the UK, to ensure they are able to

- Abide by the countries data protection / restriction policy
- Access the service (365 / Canvas) in the country they are planning to visit (see line highlighted in yellow above)

Removal of any encryption software and encrypted data from laptops or mobile devices will need to take place or application for the appropriate licence well in advance before leaving the UK.

Note: All Microsoft Online Services are unavailable in Cuba, Iran, Democratic People's Republic of Korea, Sudan, and Syria.
Some countries with encryption restrictions are: China, Morocco, Russia, Cuba, Ivory Coast, Iran, and Iraq.

Introduction of the policy to students
Students will be required to accept the guidelines for acceptable use of ICT and digital devices as part of their induction to the School and also every time they log onto a School computer, laptop or other equipment. They are not able to log on unless they agree to the terms set out on the log on screen.

A module on responsible internet use is included in the Computing curriculum covering both School and home use. This module will include password awareness, cyber-bullying and e-safety and are part of the Computing and PSHE schemes of work.

Informing staff
All staff including teachers, classroom assistants, supply staff and support staff, will be required to accept the terms of the Acceptable Use of Digital Devices Policy before using any ICT resource. Staff will be made aware that internet traffic is monitored and traced to the individual user and machine and that discretion and professional conduct is essential. Failure to follow the Policy will result in disciplinary action. Reminders are sent to staff at regular intervals. Visitors are not usually allowed access to School ICT systems, although limited access is given to some trainee teachers, at the discretion of the Headteacher.

Informing Parents/Carers
Parents'/Carers attention will be drawn to this policy on the School website. Parents will be required to read the guidelines for acceptable use of the School's ICT systems with their child and sign the agreement. A partnership approach with parents will be encouraged. Information on 'cyber-bullying', 'safe use of the internet' will be published on the School's website and MLE *(Canvas / Microsoft Office 365)*. A copy of this policy can be found on the Rooks Heath website. Further information is given to parents/carers on admission to the School, as part of the induction process.

Sanctions for the misuse of the internet facilities and digital devices
There may be a temporary removal of access to the School network for a fixed or unlimited period if students misuse ICT facilities. There may be occasions when the police may need to be contacted. Depending on the nature of the incident, sanctions for misuse or irresponsible use include bans from using the School's ICT

facilities, seclusions and exclusions in accordance with the School's Behaviour for Learning policy. Parents will be charged the cost of replacement that is needed because of any wilful damage by their child.

Staff are expected to have high standards of ICT use and will face disciplinary action if they abuse the rules concerning the use of this. This includes the use *anywhere* they use School ICT equipment. *Securus* monitors staff use of School ICT equipment, even offsite. The Deputy Headteacher, Pastoral gives regular reports and, over time analysis, to the Headteacher of misuse of the ICT systems by students. Staff incidents are reported immediately they are discovered.

Leavers

When students or staff leave the School, their accounts will disabled by ICT support as soon as is practicable and no later than after two weeks. Information about leavers and joiners are communicated to the ICT support team as part of the communications system. In the case of users facing disciplinary action, this will be immediate. This information is communicated to the ICT support team by the Headteacher, Director of Business or the PA**.** Emails will be archived and data will usually be kept for a minimum of 7 years. This data is securely kept by ICT Support and is accessible to the Headteacher or Director of Business if required.

Extended Assurance

The School's ICT systems and relevant policies are checked at regular intervals.

The School follows the requirements, as set out by ESFA in the Academies Financial Handbook, to undergo a process of review and scrutiny of processes and governance of its ICT systems and procedures. This is largely done by the Headteacher, Director of Business, the E-Learning Administrator, Head of Computing and the Network manager. The ICT systems and processes are subject to review by the School's auditors according to the work programme agreed by Governors and once a year at the annual audit.

Appendixes

Appendix A
Acceptable Use Contract is the School's Acceptable Use of Digital and ICT Devices contracts for both students and staff.

Appendix B
Student Laptop Agreement Form is the School's form that is completed by students if they have occasion to use a School Laptop or other digital device.

Appendix C
Incident log form is the School's incident log form. This will also be logged in the School's Behaviour for Learning system.

Appendix D
Acceptable use of Digital and ICT devices – Staff contract is the form staff sign before they can access the School's digital devices, including School mobile phones.

Appendix E
Acceptable use of Mobile Phones issued by the School outlines the expectations of staff who use School mobile phones.

Appendix F
OSA Mobile Phone Log is a record of the use made of the School mobile phone used for Off Site Activities

Appendix G
Data Protection Impact Assessment (formulated with Judicium and Cloud Design Box for the implementation of Microsoft Teams/ SharePoint as part of the Microsoft 365 Suite)

Appendix A
Acceptable Use Policy
This is valid for ALL users of the system.
This Acceptable Use Policy will help protect all users by clearly stating what is acceptable and what is not.

1. Anyone using RHS ICT systems will adhere to the ICT policy or face relevant disciplinary measures.

2. Computer access may only be made with the user's authorised username and password, which must not be given to any other person.

3. School computer and Internet use must be appropriate to a pupil's education or to staff professional activity. Files stored locally must be those related to School business.

4. Copyright and intellectual property rights must be respected.

5. Users are responsible for e-mail they send and for contacts made. E-mail should be written carefully and politely. Communications by e-mail are not secure and as such, should be regarded as public property.

6. Pupils must never give out personal details such as name, address, age or telephone number. Any unsuitable communications received must be reported to a member of staff immediately.

7. Use of the network to access or send inappropriate materials such as pornographic, prejudicial, racist or offensive material is forbidden. Anonymous messages and chain letters must not be sent.

8. Staff should abide by the School policy on data protection when dealing with sensitive data.

9. The attempted use of proxy servers to bypass School internet restrictions is not allowed.

10. Use for personal financial gain, gambling, political purposes or advertising is forbidden.

11. The integrity and security of ICT systems must not be compromised. Any form of hacking or accessing restricted files will not be tolerated.

Irresponsible use may result in being banned from the internet or loss of access to all School computer systems.

The School will exercise its right to monitor the use of computer systems, including the monitoring of internet use, interception of e-mails and the deletion of inappropriate materials at all times. In circumstances where the School believes unauthorised use of the computer system is, or may be taking place, or the system is, or may be, being used for unlawful purposes, the School reserves the right to inform appropriate authorities and provide documentary evidence. Internal procedures also follow.

*Signature:*_____*Date:*_____

Appendix B **Student Laptop Agreement Form**

Introduction.
This agreement has been drawn up to set the conditions by which a student may have personal use of a School laptop computer, be it supplied directly by the School, or via any other laptop funding scheme. The Student Laptop Agreement Form is set out to inform all of the conditions under which they may have the use of a School laptop computer, and is intended to guide and protect both the student and the School.

In order to effectively administer all of its computer systems against attack by viruses, spyware and hackers, the School reserves the right to scan, review and delete any files that may be held on its computer systems, including laptops. This may at times necessitate the monitoring of an individual's computer and/or internet activity. In any circumstances, personal privacy and confidentiality will be strictly observed at all times.

Student Laptop Acceptable Use General Statement.
The agreed conditions under which a Rooks Heath laptop computer is allocated to a student use by Rooks Heath School include, but are not limited to, the following;

- I accept personal responsibility for all use of the Laptop Computer issued to me.
- Every care and consideration will be made by myself to look after and protect the laptop which has been supplied to me for my personal educational use by the School.
- Laptop use should be appropriate to personal education or staff professional activity.
- Computer and Internet access should only be made through my own login, which should not be made available to any other person.
- I understand that as the laptop will regularly be attached to the School's computer network, every care must be taken to prevent it becoming infected with any computer viruses or other malicious software which it might then pass on. To this end, I will undertake to;
    1. Regularly update the definitions utilised by the laptop's pre-installed Anti-Virus software and Anti-Spyware applications, if applicable. (see point 3)
    2. Regularly perform a Windows Update to keep my laptop protected with the latest patches, fixes and software updates. (see point 3)
    3. Where it is not possible to undertake points 1 and 2 myself, I will regularly return my laptop to the ICT Support team so that they may undertake the required operations for me.
    4. Refrain from using any personal device such as a mobile phone as a 'hotspot' to provide access to services outside of the School network.
- In any case, when requested, I will return the laptop to the ICT Support staff so that a general health check and service can be undertaken upon it.
- I will immediately report any problems or concerns found with the laptop to the ICT Support Team.
- No files shall be downloaded from the Internet unless directed by the teacher in charge of the lesson.
- Any special conditions listed below will be observed and strictly adhered to.
- Use of the laptop to access inappropriate material such as pornographic, racist or offensive material is strictly forbidden.

Special Conditions for Student:
I understand that laptop computers are extremely vulnerable to theft and special care must be taken to keep them safe. In particular, it is recommended that they are not left openly on display in a vehicle or even at home!

1. I will not allow any other student to use the laptop at any time.
2. The Rooks Heath site insurance only covers the laptop whilst it is on the School's premises. It does not cover it in your home, at another site or whilst being transported to and from Rooks Heath.
3. Students granted the use of School's laptops are now held personally accountable for their damage at all times, and their loss or theft when away from the Rooks Heath School site, and will be expected to fully reimburse the School with the cost of a repair or replacement should their laptop be damaged, lost or stolen.
4. I understand that laptop computers are extremely vulnerable to theft and special care will be taken to avoid leaving my laptop in public view, either in a vehicle or even at home.
5. When the laptop cannot be with me, e.g. during PE lessons, it will be left safely with a member of staff.

By signing this form, I confirm that I have read and agree to abide by these acceptable use rules and special conditions for use of a Rooks Heath School laptop computer. Irresponsible use may result in being banned from the internet or loss of access to all School computer systems.

***Students Full Name:*_____**

***Date:*_____**

***Students Signature:*_____**

***Tutor Group:*_____**

Parent/Carer Permission.
As the parent/carer of the student signing above, I agree to the terms and conditions above and grant permission for the student to have the use of a School's laptop computer during their time at Rooks Heath School. I understand that students will be held accountable for their own actions.

Parent/Carer *Signature:*_____*Date:*_____

Student laptop agreement form

Appendix C – E-Safe Incident log form

The School will keep an incident log and monitor the measures put in place. This will enable the School to know that the students are e-safe.

DATE: ……..

TIME: ……..

INCIDENT LOGGED BY: ……..

STUDENT(S) INVOLVED: ……

DETAILS OF THE INCIDENT:

DATE WHEN PARENTS WERE CONTACTED (if a student): ……

ACTIONS TAKEN:

ADDITIONAL COMMENTS:

Entered into E-Behaviour by: …….. ……

Role: …….

Signed: ……. Date: ……..

Appendix D

Acceptable use of Digital and ICT devices – Staff contract

The computer network, School funded laptops and mobile phones are owned by the School and are made available to staff to enhance their professional activities including teaching, research, administration, communication and management. The School reserves the right to examine or delete any files that may be held on its computer network, laptops or mobile phones to monitor any Internet sites visited by staff.

Members of Staff should regard the following guidelines for 'Acceptable use of Digital and ICT systems' as part of the School Staff Handbook and are required to comply with the guidelines.

1) All Internet activity should be appropriate to staff professional activity or students' education; If staff discover any unsuitable sites, the URL (website address) and content must be reported to the network manager who will arrange for its exclusion from future access;
2) Access to the network should only be made via the authorised username and password, which should not be made available to any other person;
3) Activity that threatens the integrity of the School ICT systems, or activity that attacks or corrupts other systems, is forbidden;
4) Members of Staff are responsible for email sent and contacts made that may result in email being received;
5) Use for personal financial gain, gambling, political purposes or advertising is forbidden;
6) Copyright of materials must be respected and sources acknowledged when used;
7) Posting anonymous messages and forwarding chain letters is forbidden;
8) As email can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
9) Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden;
10) Staff should not run social network spaces for students on a personal basis.
11) Staff should not give out their mobile number or home phone number to students or parents. Staff should not use their personal phone or camera without permission e.g. for a School field trip. If personal equipment is being used it should be registered with the School and a clear undertaking that photographs will be transferred to the School network/MLE and will not be stored at home or on memory sticks and used for any other purpose than School approved business.
12) School laptops must not be left in an un-locked room.
13) Staff with responsibility for managing and accessing personal data in the School's Management Information System (Capita SIMS), the MLE (Canvas / Microsoft) or online reporting (MCAS), will comply with the following conditions:

a. The data is to be used only for educational purposes.
b. Personal data is to be shared only with those who need the information to discharge a statutory education function.
c. Only authorised users may access the system and they must never share their login details with anyone.
d. Management of Canvas / Microsoft usernames and passwords is the responsibility of the authorised system manager/MLE administrator in the School.
e. Care will be taken to protect any data which is printed or otherwise displayed.
f. Temporary data sets will be deleted as soon as possible.

Signed: …….. Date: …….

Name (Block Capitals): ……

Appendix E

Acceptable use of Mobile Phones issued by the School

The following requirements relate to mobile phones and are in adremovedition to those listed and agreed in the ICT Acceptable Use Policy.

Mobile devices are configured to standard builds and tariff bands before delivery to the user. The School will monitor individual usage through itemised billing.

Issued mobile phones are for School business use. Usage should be reasonable and justified in relation to work. It is accepted that on some occasions personal usage may be necessary. This should be reasonable, not excessive and arrangements should be made to repay the costs of personal use if these exceed the monthly tariff.

It is the responsibility of the Finance Manager to check itemised bills, ensuring that call volumes and costs are appropriate and not excessive (for work purposes as well as any personal use). Where a user cannot justify call usage and costs on a repeated basis, it is the discretion of the Head Teacher or Director of Business to initiate disciplinary action in line with the Staff Disciplinary Policy.

Calls between the School mobiles are free. In order to help achieve best value for the School, staff issued with a mobile phone are expected to call these numbers from their mobile phone and not from a School landline. Therefore, these numbers should not be distributed to staff. Contact should be made via Reception in the usual manner.

School property

School purchased and leased mobile devices are School property (regardless of the source of funding). They are not a user's personal property nor are they available for individual resale or remuneration. All School purchased and issued mobile devices must be returned to the School upon termination of employment or on request. The School will securely erase data on mobile devices and reformat the device before re-issue to another School user. The device will also be securely erased when disposed of at the end of its lifecycle.

Reporting loss or theft of device

In the event of loss or theft of a mobile device the user should immediately report any theft to the Police and then inform the Operations Manager. In relation to theft or loss of a mobile phone the user should also notify the Mobile provider directly on Tel: 0800 977 7337 or at http://service.o2.co.uk/IQ/srvs/cgi-bin/webcgi.exe?New,KB=Companion,T=contact_Us_Business

Signed: …….. Date: …….

Name (Block Capitals): ……

Appendix F OSA Mobile Phone Log

Date of Trip and date of Mobile taken	OSA destination	Trip leader	Calls made	Texts

Appendix G
Data Protection Impact Assessment Extract

(Formulated with Judicium, Cloud Design Box and Rooks Heath School for implementation of Microsoft Teams/ SharePoint, 2020)

The (Microsoft SharePoint/ Teams) system is cloud based so the data is held on a Microsoft data centre. This means that the School cannot "protect the data" independently. Mitigation of risk is created through the systems used to minimise access to only those who have the appropriate level of authority to access required data and for changing access.
(A significant number of Teams have been created on Microsoft Teams to minimise access to data. All access requests to a specific Team need to go through the Network Manager).

Data is technically accessible from anywhere with an internet connection meaning the protection of data is the responsibility of each user (e.g. lock machine when unattended, minimise downloading files to their personal local devices etc)
(Professional Development is delivered to staff in these areas as part of the move to SharePoint/ Teams. When new staff join Rooks Heath, this is also covered in the new staff induction day).

Steps taken to protect data by a) Cloud Design Box, b) Rooks Heath School:
a) Once data has been uploaded to Microsoft 365 it has Microsoft defined encryption / versioning and backups. As all data is currently stored in their Office 365 tenant, so they already have procedures and security measures in place to protect the data.

Cloud Design Box products extract the information from the school MIS and then update RHS's other systems in the manner the School have requested. It is not stored elsewhere or held apart from in memory except in the following circumstances:

1. If RHS have asked explicitly for it to be stored elsewhere e.g. a list of new accounts.
2. As a temporary measure during installation or support. After which any temporary stored data is deleted.
3. Log files could contain some personal information.
4. If required to be passed to a different computer for processing.

The following measures are in place by Cloud Design Box:

1. Information is extracted from the MIS using the APIs provided by the MIS supplier, or in the absence of them, by reading the database. Cloud Design Box uses the credentials that the school provides and depending on the MIS provider and their security model, can only access the information that you give us access to.
2. When accessing a hosted MIS or 3rd party system they will always use industry standard SSL encryption where available. Passwords are encrypted and are not stored in clear text.
3. The information from the school will only be held within the school's systems and will not be transferred to any of their systems or machines.
4. Cloud Design Box provide Data Protection Legislation training to all staff to ensure they follow the internal processes and polices to ensure all data processed is Data Protection Legislation compliant. All staff and subcontractors have enhanced DBS checks.

The following security processes are in place by the School:
The school's ICT policy is to be followed. The policy encompasses the security by:

- Ensuring user passwords aren't forever static ensures the SharePoint / Teams credentials do not remain the same.
- Passwords have forced complexity (passwords must meet a minimum complexity criteria)
- Users are encouraged to adhere to the principles identified by the policy as follows:

"Access to School ICT systems may only be made with the user's authorised username and password, which must not be given to any other person. Passwords for all users will be reasonably complex and will be at least alpha numeric and subject to at least annual change."

Duration of processing: Cloud Design Box will continue to process MIS data while there is a valid license and contract in place unless otherwise requested by the Data Controller. Data is processed in batch jobs which can run several times a day to sync the data.

Termination: On termination of a valid license and contract for any reason or expiry of its term, Cloud Design Box will securely delete or destroy or, if directed in writing by the Data Controller, return and not retain, all or any data which may be in its possession or control.

Third parties: School data is only held within our own systems (SIMS, Active Directory and Office 365) and will not be transferred to any of Cloud Design Box's systems or machines.
Cloud Design Box will only process other data by written instructions from the Data Controller.