ACKLAM GRANGE SCHOOL

AGS Digital Handbook

Status & Review Cycle	**Term**	**Year**
Last Review Date	Autumn	2024-2025
Next Review Date	Autumn	2025-2026
Lead SLT	Mr Lodge	

This school is an academy within The Legacy Learning Trust.

The Legacy Learning Trust

Contents

1. IT Service and Development Team

The team is based on the 1st floor in the Admin Block. They administrate, monitor and maintain the servers and all IT hardware and software across the school. They also provide IT support for staff, students and visitors across the school both in the classroom and outside. This includes assemblies, events etc. A key focus of the team is to research, develop and implement emerging technologies that can be used in the classroom to further develop the learning experience at Acklam Grange School. If you have a technical issue with any aspect of IT that needs attention in some way then you should put in a support call by emailing helpdesk@tllt.org.uk

The makeup of the team is as follows:

TLLT IT Manager – Mike Lodge
Senior IT Service Engineer – Andy Fletcher
IT Service Engineer – Mike Johnson
IT Service Engineer – Taylor Robinson

2. Adding to the AGS Digital Handbook

If at any time you think there could be a useful addition to the Digital Handbook, please liaise with Mike Lodge (IT Service & Development Manager) to see if its inclusion is appropriate.

3. Communication: Parents/Carers

It is acceptable to communicate with parents/carers on educational matters using your school email account however telephoning home is the primary method of communicating with parents. You should always keep copies of any emails that you send to parents. Please ensure that appropriate language and tone are used and established communication protocols are adhered to. Do not communicate with any parent/carer using your personal email account, a social networking site, or your personal mobile telephone. In some instances, e.g. on a trip in an emergency situation, the use of a personal mobile telephone may be acceptable. Centralised communications with parents/ carers can be made using the electronic system SIMS InTouch which enables selected data held in SIMS to be automatically emailed (or texted) to parents/carers. This feature will be used to send out documents such as Student Reports, Attendance Reports, Pride Reports etc. and will be centrally managed by the Data Team.

4. Communication: Students

Do not communicate with any student using IT unless it is work-related. You must establish safe and responsible online behaviour. Do not communicate with students on any social networking site. All communications must take place within clear and explicit professional boundaries. You should not access social networking sites of students; do not give any student any of your personal contact details, including your mobile telephone number. Never send any student personal messages. Contact with students should be limited to email, Class Charts, or SIMS InTouch. There may be rare occasions when going outside agreed protocols is absolutely necessary; on such occasions a member of the Senior Leadership Team should sanction it.

5. Consumables

Consumables cover such items as toners, paper etc. We have a print management solution that means toner is replaced automatically by the Admin Team when it runs out. Paper for the Multi-Function Devices (MFDs) is also replenished by the Admin Team. If paper is required for a classroom or office printer then please telephone the Admin Team on extension 4000. Please refer to the section on ‘Printing’ for further information. Departments and other cost centres will receive a one-off charge at the start of the financial year to cover the cost of consumables. This charge is monitored on a yearly basis and is dependent on the previous year’s usage.

6. Copyright and Intellectual Property Rights

All materials that are saved on any of our IT systems must follow copyright and intellectual property rights. If you are in any way unclear or unsure as to if such rights are being adhered to, please liaise with Mike Lodge. You may find the following web links useful:
http://www.ipo.gov.uk/types/copy.htm
http://www.staffs.ac.uk/legal/copyright/what_is_copyright/

7. CPD – IT Related

Specific identified whole school IT training needs are catered for through AGS Inspire, our professional development programme which delivers sessions every Tuesday from 4.00pm until 5.00 pm.

8. Cyberbullying

This is where IT is used deliberately to cause someone harm, distress or upset. There are some unique features of cyberbullying less present in more traditional forms of bullying – the immediacy, the absence of interactions, the absence of a safe home environment and the anonymity. As part of our Pay and Conditions of Service, it is our duty to ensure, as far as possible, that students are free from bullying and harassment – cyber or otherwise. If you become aware of any student involved in cyberbullying using hardware owned by the school, their own mobiles device, or from/at home, then this should be reported immediately to the relevant Year Leader or a member of the Safeguarding Team.

9. Data: SIMS and School Databases

All such data is strictly private and confidential and as such we all have a duty of care to ensure that it is used and accessed safely. If you are accessing SIMS from home, please ensure you are the only individual privy to this data and do not leave such data unattended. This also applies to the work place i.e. do not leave a PC unattended where other individuals (e.g. students, visitors, parent/carers) could see such data. No personal data (staff or student) should be taken from the school unless it is on encrypted media. This includes, but is not exclusive to, laptop computers, netbooks, external hard disks, memory sticks, smart phones and other removable media. No school related data, documents or images should be stored on personal computer devices under any circumstances.

10. Data Security

Staff computers are set to lockout after 5 minutes of inactivity as a security feature. Please note that you will need to log off your PC to make it available to other users, otherwise it stays locked in the first user's name and cannot be unlocked by the new user coming into the room. If you have sensitive data on your PC and you need to step away for a short while you will need to lock your computer quickly by pressing the “Windows logo” key and the ‘L’ key together. Please do not hesitate to contact the IT Service and Development Team if you need any further advice.

11. Email: Work

We have our own school email system that uses Microsoft Outlook as part of Microsoft Office 365. This is our default internal communication method between staff. You are advised to check your e-mail account at least twice a day. The system should be used for all communications – internal and external of a work-related nature. Please use the school e-mail appropriately; this includes language and tone. On occasion it is not appropriate for all staff to be sent certain information and ‘forwarded’ e-mails to others, i.e. forwarded e-mails that include the whole thread. There may be times when you receive information that you may view and at first glance you may question its relevance to you; please be mindful that such information may prove very useful in unexpected circumstances. The school e-mail system has many ‘group lists’ already set up within it to make communications quicker for you e.g. AAA All Staff, AAA Faculty Leaders, AAA Year Leaders etc. If you have any additional groups that you believe would be useful for you or others then please log a call.

12. **Email: Personal**
    Access to your personal email account is acceptable, but only outside normal working hours. However, you must ensure that any content viewed is appropriate to a workplace setting where children and young people and other colleagues are present. Do not open any attachments from unknown sources as you may put the school network at risk. Please be aware that the Securus system is monitoring your activity and may pick up confidential personal information.

13. **E-Safety Promotion**
    Please ensure you promote e-safety with any child or young adult in your care. All staff have a duty to promote e-safety wherever possible. Students should be encouraged not to give out their personal details on any social networking site or in any e-mail. If you become aware of any such incident, please inform the relevant Year Leader or a member of the Safeguarding Team. Please refer to the E-Safety Policy for further information.

14. **Extremism and Radicalisation**
    Individuals, groups and organisations with extremist and radicalised views use the internet to exert influence on young people. Staff and students are prohibited from accessing any websites or social network pages that promote such views. The school has systems and filtering in place to block extremist material and to monitor those who attempt to access it. Any persons deemed to be accessing extremist material will be reported to the relevant authorities. Refer to the school's Safeguarding & Child Protection Policy for more information.

15. **Hardware**
    Hardware relates to any piece of IT hardware owned by the school i.e. PCs, monitors, hard-drives, interactive whiteboards (IWBs), digital projectors, printers, visualisers and any other portable IT devices such as laptops, tablets, digital cameras or mobile phones. All hardware owned by the school should be used for work-related purposes by staff and students. As stated, some occasional personal use of email and the internet is acceptable (but refer to advice in this document as to what is acceptable). All hardware should be looked after and this includes ensuring that all IT equipment is turned off at the end of the working day.

16. **Hardware: Damage**
    If you become aware that any item of hardware has become damaged, it should immediately be reported to the IT Service Team by emailing helpdesk@tllt.org.uk. This will ensure that there is no health & safety danger to staff or students and that the equipment is returned back into service as quickly as possible. Staff should be aware that the cost of replacing and repairing IT equipment is high and therefore a high level of vigilance is required when teaching in an IT room or when using IT equipment to alleviate the amount of damage that occurs.

17. **Hardware: Disposal**
    No item of IT hardware should be 'thrown away', even if you think it is old and no longer used. The school must follow government guidelines to ensure the safe and appropriate disposal of such items. If you become aware of an item that you believe to be of no more economic use, this should be communicated to the TLLT IT Manager who will make the appropriate arrangements.

18. **Hardware: Lending**
    Do not lend any piece of hardware to a student to take home for use. Under certain circumstances it may be possible, but this should be agreed with the IT Service Team and appropriate records kept.

19. **Hardware: Purchase**
    All pieces of IT hardware should be purchased via the IT Service and Development Team, even if the central IT budget is not financing such a purchase. This ensures that appropriate checks related to suitability are made prior to purchase and that subsequent procurement, delivery, storage, security marking and installation protocols are followed.

20. Hardware: Relocation

No member of staff should attempt to relocate or move any non-portable piece of IT hardware. Non-portable devices can only be relocated by a member of the IT Service and Development Team, due to reasons of insurance and health & safety. The IT Service and Development Team maintain a detailed inventory of where all IT hardware is located. If anyone relocates an item, they compromise the integrity of that inventory and this could create real problems related to health & safety and/or insurance.

21. Hardware: Security

All steps should be made to take good care of all items of IT hardware owned by the school. Portable devices should be locked away when you do not have direct sight of them e.g. laptops.

22. Hardware: Staff Laptops

Staff wishing to undertake school work at home are expected to use the remote access function via a home computer. Each department also has a provision of staff laptops that can be booked out and taken home. Please speak to your departmental lead if you wish to do this. Laptop users must ensure they update their virus protection at least monthly by ensuring that their laptop is brought into school and logged into the network.

23. Hardware: Taking off-site

There may be times when it is appropriate for members of staff to take pieces of IT hardware off-site. On such occasions the appropriate permission must be obtained. This involves communicating with Mike Lodge and the completion of relevant paperwork.

24. Information Screens

There are a number of large TV screens situated around the school site. We use these screens as one of our means of communicating with students; namely for relaying key information to them for the day, upcoming events and activities and as a means of sharing and celebrating their individual successes. Content to be displayed on the screens should must be approved by SLT.

25. Internet – Filtering

In school we use a Smoothwall web filtering system to control and monitor use of the internet. The system is closely tailored to the specific needs of our school. Smoothwall filters and analyses the content and context of new material in real time to prevent anything inappropriate from slipping through. Any device connected to our Wi-Fi is filtered and protected, including: iOS, Android, Blackberry and Windows. Please be aware that HTTPS traffic is decrypted and analysed to allow the filtering of secure sites. This data is not readable at any point. For more information or support please contact a member of the IT Service and Development Team.

26. Internet: Staff

Using the internet on any piece of IT hardware connected to the school should be done for work-related matters. You cannot use the internet (on any piece of our hardware) for: gambling, accessing pornography and/or indecent images, accessing extremist material, to incite any form of discrimination, to conduct any personally run business matters, share dealing, religious and political causes or beliefs, playing games, harassment or accessing social networking sites. Some occasional use of the internet for non-work related matters is acceptable outside of school hours. However, it is important to note that all such activity is monitored and disciplinary action could be taken if the school deems such activity to be inappropriate or not covered by our Guidance for Safer Working Practices for adults who work with children and young people in education settings.

27. Internet: Students

Students have to sign an Acceptable Use Policy (AUP) before accessing the internet. If you become aware that a student is using the internet inappropriately, please report it to the IT Service and Development Team or the Safeguarding Team. Inappropriate use follows the same guidelines as for staff. Students should not be accessing social networking sites.

28. Wireless Access: Students

Students are able to connect to the school wireless using their personal devices. The access provided to students is limited to sites identified as important to the students' education. This includes Office 365, Class Charts etc. If you would like students to have access to a particular site please contact Mike Lodge to discuss.

29. Websites

There are many occasions when you may wish to access a particular website to facilitate learning and teaching. On such occasions, all such content should be related to the curriculum and appropriate to the age group concerned. If you need advice as to whether a particular site is appropriate, then please liaise with your Faculty Leader. In short, students should not be exposed to unsuitable material or web-links on the internet. You must not access the internet for personal use in lesson time.

30. iPads: Bookable Resource

In school we have three sets of iPads that are available to book via the School Booking System which can be accessed from your computer Start Menu. Choose 'IT Resources' from the menu and you will be able to check if a set (or more) of iPads is available when you require them. If they are then please email helpdesk@tllt.org.uk to get a member of the team to enter your booking on the system. The iPads have a wide range of Apps already installed but if you would like to use a different App then please contact a member of the IT Development Team to discuss what is possible.

31. Monitoring

All activity on our IT systems is monitored using our Securus system. The school is aware that the interception and monitoring of electronic communications is unlawful. It is lawful if the sender and recipient are aware that such monitoring will take place and/or there are lawful exemptions that will prevent or detect a crime and/or we need to investigate or detect unauthorised use of the internet. Therefore, this document acts as a means of communicating to you that such interception and monitoring will take place. Where we become aware that guidelines in this document are not being adhered to and there is misuse, we will adopt the Middlesbrough Personnel Procedures. These procedures cite that most serious misconduct activities can lead to disciplinary action and possibly dismissal. The monitoring of staff activity is scrutinised and managed by the Headteacher.

32. Personal Privacy (internet and emails)

You cannot expect absolute privacy on any IT system within the school. Monitoring takes place through the Securus system, so please bear this in mind when using our IT systems.

33. AGS Printing Strategy

In September 2017 we introduced a new printing strategy into school with the aim of making staff and students **'Think before you Print'**. We want all of our users to be more intelligent about their printing and only print if that is the most appropriate (and cost effective) method available. The strategy is based on the fact that there are a number of alternative ways of communicating information for both staff and students. This includes email or Class Charts messages with attachments, SIMS InTouch, Magellan etc. Full details are available in the document **'AGS Printing Strategy & Guidelines'** which should be read by all staff. The document includes comprehensive guidelines for student, teaching staff, support staff and admin staff printing and copying.

34. Print Management System

We have a number of Multi-Functional Devices (MFDs) that use 'Follow Me' technology. You will need to be issued with a 'Mifare Card' from Student Services before use. There are a number of additional printers in faculties around school. All printers are monitored for usage. Toner is replaced automatically, except for a handful of standalone printers. Please contact IT support for further information.

35. Multi-Functional Devices

These are large devices that allow you to print and photocopy in both mono and colour on page sizes A3, A4 and A5. They also have additional features such as the ability to scan and photocopy. They also have an auto feed facility to help with copying large documents. To print to an MFD you need to select 'Follow Me Printing' from the print menu. Printing should be restricted to work-related matters and not for personal purposes.

36. Projectors: Replacement Bulbs

Some digital projectors give warnings as to when bulbs are going to reach capacity. In these circumstances, please immediately refer it to the IT Service Team by logging a call. The IT Service Team will make the necessary arrangements to ensure a replacement is installed or if necessary purchased as soon as possible. Some older models do not give any warning, so please be aware that some disruption to your use may occur. We will continue to look at ways to minimise such disruption. Please turn off projectors when not in use.

37. Projectors & Interactive Screens: Turning Off

Staff should ensure that all digital projectors and interactive screens are turned off when they are not in use, or at the end of the day. You will compromise their use if you do not follow this advice. Please also ensure that all computers and monitors are appropriately logged off and shut down when not in use and at the end of the day. Once again, if you do not, you compromise their use in terms of reliability, but also it can present a security risk in our non-working hours.

38. Remote Access

Staff have the facility to access their school network folders from home using either Ericom Access Now. Ericom Access Now is for staff only and provides a remote desktop solution.

It is essential that you follow the guidelines in the school E-Safety and Data Protection policies when accessing confidential and sensitive information and data. If you are accessing SIMS from home, please ensure you are the only individual privy to this data and do not leave such data unattended. No confidential or sensitive data should be saved to a local IT device outside school. When you have finished, remember to disconnect from remote access.

39. Reporting Misuse

Should you become aware that there has been a departure from the various guidance sections in this document, you should report it immediately to the TLLT IT Manager (Mike Lodge) who will deal with it directly or escalate the matter to the Head Teacher as appropriate. Obscene material involving children will be reported to the police.

40. Reporting Inappropriate Material

Should you see any material that is inappropriate on any of our e-communication tools, e.g. the school website, information screens etc., you should report it immediately. You should detail what you have seen (text and/or images) in a written email to Andrew Hassack. Corrective action can be taken immediately. Obscene material involving children will be reported to the police straight away.

41. Sanctions

If you become aware that a student has engaged in anything that is clearly unacceptable (as detailed in our Student Acceptable Use and Safeguarding & Child Protection policies), you must follow it up using our standard procedures (as detailed in our Behaviour Policy). There are occasions when certain behaviours need to be reported to the TLLT IT Manager (Mike Lodge) and/or an appropriate member of the Safeguarding Team.

42. Saving Files

Files should be saved either on our network, or to your OneDrive which you can access via Office 365. When saving on the network, documents related to yourself should be saved to your home folder ('Documents'); files that you wish to share with other staff should be saved in the 'RM Staff folder'; files to be shared with students should be saved in the 'RM Shared Documents' folder. Both 'RM Staff' and 'RM Shared Documents' have been set up with a 'locked' folder structure at the top levels so as to maintain the integrity of the structure. 'RM Staff' also has access permissions placed both on individual folders and sometimes files to ensure access to files is appropriate. If you need to change the access rights on a folder/file or create (or delete) a folder then please contact the TLLT IT Manager (Mike Lodge) to discuss what you need.

43. Scanning

If staff or students need to scan a document then you should use the Multi-Function Devices which are located in every block in school. Staff are able to scan either to a USB drive, to email, or to the 'SCANNED' folder in RM Staff. Please note that if you scan a sensitive or confidential document you should move it to your own folder as soon as possible as it can be viewed by all staff. Files remaining in the 'SCANNED' folder at the end of the day (12pm) are automatically deleted for security reasons.

44. School Website

Our website address is www.acklamgrange.org.uk. The school website is a very useful communication tool for parents/carers, students, governors and staff as well as any other interested parties. Please contact the school marketing manager (Beth Hart) if you would like to publish information on the website or if you notice that something is missing or out of date.

45. Software: Copying

School licensed software must not be copied; making copies without permission is an infringement of copyright law.

46. Software: Installation

You should not install or attempt to install any piece of software on any piece of IT hardware owned by the school. It must be referred to the TLLT IT Manager. This will ensure that the appropriate safeguards and licensing arrangements are in place.

47. Software: Licences

These are held centrally by the IT Service and Development Team. They should not be held by individuals or within departments/faculties.

48. Software: Purchase

It is acceptable to purchase new software from individual/department/faculty cost centres but, the purchase should only proceed if the software has been deemed appropriate by the IT Service and Development Team. The team maintains a software register.

49. Staff IT Acceptable Use Policy (AUP)

All staff are required to carefully read, sign and return the AUP at the start of the academic year or, if new to the school, as soon as they start working at Acklam Grange School as part of the induction process.

50. Student IT Acceptable Use Policy (AUP)

All students must read and sign the appropriate AUP (KS3 or KS4) before the student is allowed to use the school computer network and internet. Staff should support the contents of the AUP and promote its positive application. Copies of the AUPs can be found in the RM Staff folder and on the school website. Staff should communicate this with their tutees. New students will follow the above procedure as part of the induction process which will ensure that the student fully understands the implications of the document. Please also read the 'Sanctions' section for further guidance in this area.

51. USB Storage Devices

USB devices can be used within school but they do present a risk both in terms of data and virus protection. Where possible staff should use alternative, cloud-based methods, such as OneDrive, to save work. Alternatively, they could use the Ericom Access Now remote access solution to access the school network drives. Any USB storage devices containing school data must be encrypted and virus checked before being used within school.

52. Usernames and Passwords: Staff

Usernames and passwords are needed to access most IT systems in the school – SIMS, Office 365, the curriculum network, remote access etc. If you have any issues with login details please put in a support call by emailing helpdesk@tlt.org.uk. In cases where you set your own password, **a strong password** should be used. A password should be a minimum of 8 characters in length, contain upper and lower case alphabetical characters and numbers or punctuation characters. It should not contain your name, date-of-birth or other readily available personal information. Passwords should not be easy for others to guess. It is an offence under law to access or use another person's username and/or password. Do not let anyone else, particularly students, use any of your usernames and passwords on any system.

53. Usernames and Passwords: Students

Usernames and passwords are needed by students to access the curriculum network, and Office 365. If for any reason a student does not have a username and/or password for these systems, they should be directed to the IT Service and Development Team. Students should be encouraged to set passwords that are easy for them to remember but not easy for others to guess – they should try to ensure passwords contain a minimum of 8 characters, contain upper and lower case alphabetical characters and numbers or punctuation characters. It is against our student Acceptable Use Policy for any student to access or use another person's username and/or password and students will be told not to let anyone else use any of their usernames and passwords.

54. Viruses

We have relevant protection in place, but due to the nature and emergence of viruses, some can find their way onto our networks. If you are using removable devices, always run a virus check before you access saved files to ensure that no virus is on them. If there is, immediately disconnect and refer the issue to the IT Service and Development Team.

Key Software

SIMS

SIMS is our Management Information System and it is our primary source of data. It is used primarily to take registers, enter attainment data, administrate consultation evening appointments etc. All staff have an individual username and password. Much of the data in SIMS is confidential and potentially sensitive. To conform to the Data Protection Policy, staff should ensure that they logout of SIMS or lock the screen if they move away from their computer. When accessing SIMS remotely staff should take extreme care to ensure the data remains confidential.

Web Browsers
In school we have access to both Google Chrome and Microsoft Edge web browsers. Chrome is our recommended choice but on occasion you will find that certain applications will work better on one browser than the other. If a web application does not work then always try both browsers before requesting support.

Microsoft Office 365 (O365)
Office 365 encompasses many things including exchange-based email, calendar and contacts management. It also provides access to Microsoft's Office Web Apps; streamlined online versions of Word, Excel, PowerPoint and OneNote that can be used to view, create and edit documents. Office 365 also includes OneDrive, for online file storage and collaboration. Office 365 can be accessed by going to www.office.com

Microsoft Office
Microsoft Office is the primary suite of Office Applications software we use in school. We are currently using Office 2019 which provides access to Word, Access, Excel, PowerPoint, OneNote, Publisher and Outlook. Students or staff who do not have access to full Microsoft Office on a home device have access to the Web App versions of the software through Office 365 as long as they have an internet connection.

Ericom Access Now
Access Now is an alternative method of remotely accessing the school network and is the recommended method for use by staff. It works in a different way to Magellan and uses a 'remote desktop' which provides access to the network drives (Home folder, RM Staff and RM Shared Documents) as well as SIMS and other applications software. To access Access Now from outside school you can either click on the link on the homepage of the school website (top right) to get to Magellan and then select the Access Now – Staff Remote Access tile or you can enter https://remote.acklamgrange.org.uk into your web browser. You should use the same username and password you use to access the school network.

If you have any problems with the setup, please contact the IT Service and Development Team.

ClassCharts
ClassCharts links with SIMS to provide us with attractive seating plans for our classes which can be displayed on screen or printed out. The plans are populated with key student data thereby important information is at your fingertips. ClassCharts is also used to enter achievement or behaviour points for your students. The system allows for super-fast behaviour management support via the PSAs who receive the Activity Feed from ClassCharts which means they know immediately if there is an issue and can provide support. ClassCharts has powerful analytics which allows you to optimise your seating plans for behaviour. You can automatically create seating plans based on pupils' abilities and needs and you can even use the artificial intelligence engine to suggest seating plans that will improve behaviour in your classroom. All members of staff have a username and password to allow them to access ClassCharts – the username is your school email address. To access ClassCharts there is a tile link in Magellan or you can type https://www.classcharts.com into a web browser and enter your login details. Both students and parents have access to the ClassCharts mobile app which provides them with access to:

Students: Behaviour Score Breakdown, Weekly Behaviour Breakdown, Activity FeedParents: Behaviour Score Breakdown, Weekly Behaviour Breakdown, Activity Feed, Attendance

CPOMS
CPOMS is a cloud based software application for monitoring child protection, safeguarding and a whole range of pastoral and welfare issues in school. Working alongside our existing safeguarding processes, CPOMS is an intuitive system to help with our management of child protection, behavioural issues, bullying, special educational needs, domestic issues etc. CPOMS helps us to ensure that students are safe and fully supported, whilst school staff can focus on teaching and providing support, instead of administration. Every member of staff across school has an obligation to report any concerns which they may have. CPOMS allows you to record information in a central repository and have the relevant people alerted immediately. All members of staff have a username and password to allow them to access data in CPOMS at the appropriate level. As much of the data contained in CPOMS is potentially sensitive or confidential, access is tightly controlled and identified staff have a personal USB 'key' which provides an added level of security and allows them to access information appropriate to their role in school. To access CPOMS there is a link in the 'Start' menu on the school computers, there is a tile link in Magellan or you can type https://acklamgrange.cpoms.net/login into a web browser. For further details on CPOMS, please contact Lucy Gowland (Identified Designated Safeguarding Lead).

School Booking System
Bookings for key rooms and whole school resources are recorded in the 'School Booking System' which can be accessed from the 'Start' menu on the school computers. Actual entries can only be made by the Administrators of the system but all staff can view the bookings. To book an IT resource such as a set of iPads you should check the resource is available at the time you require it by looking at the Booking System and if it is, then you contact the IT Development Team on extension 1020 and they will enter the booking into the system.

SIMSInTouch
InTouch is a new communication tool which allows us to send out scheduled alerts and messages to our stakeholders. It allows us to send documents such as timetables, exam schedules, exam results and reports electronically to students, staff and parents using email and text messaging. It keeps a complete record of each student's details; all the responses received to text messages and emails are captured. Messages are also recorded in the student's document store so we have always got a complete record of all the students' details. InTouch is managed and administered by the Data Team.