PLANTSBROOK SCHOOL

'Be the best that you can be'

WHOLE SCHOOL ICT POLICY

Rationale

Information & Communication Technology is a loose term, which is used to describe a wide range of tools and techniques, usually electronic in nature, which speed up or ease the way in which we create, control and interpret our world and how we communicate.

All adults and students should be given the opportunity to develop their ICT capability, to use ICT to enhance their learning and become critical and largely autonomous users of ICT.

Our vision is to create an active, sustainable and flexible infrastructure for the creative and innovative use of ICT to exploit opportunities for educational achievement and cultural development. It should contribute to improving the quality of teaching and learning and enable Plantsbrook to become an e-confident and e-safe school.

1. Purposes

The purpose of the policy is to:

1. Fulfill statutory requirements to deliver ICT & Computing in the National Curriculum.
2. Provide opportunities for staff and students to develop ICT capability.
3. Provide systems to identify staff development and resource needs.
4. Provide systems to enable implementation of staff development and appropriate provision of resources.
5. Provide information on systems in place at the school, including e-mail, SIMs and disaster recovery.

2. Broad Guidelines

A management structure is in place to enable effective co-ordination, delivery and assessment of ICT:

1. A member of SLT has overall responsibility for ICT strategy.
2. There is a Learning through ICT Supporter who has shared responsibility for the development of ICT across the curriculum in all subjects, including leading on e-learning strategy.

3. There is an ICT & Computing Subject Leader who leads Teaching and Learning of discrete ICT & Computing in the curriculum.
4. There are VLE Champions (staff members) who take the lead on developing ICT within their specialism and contribute towards the development of the school VLE.
5. There is a technical support team of four technicians led by a Network Manager.
6. There is a team of Support Administrators led by the School Business Manager who use ICT systems to provide a backbone of support for school systems such as monitoring attendance and punctuality and managing assessment and reporting.

Ensuring the effective relationships between these different individuals and groups is a key aspect of the role of the Senior Leader with responsibility for ICT.

1. A basic ICT entitlement is identified for all students although it is recognised that some students will receive extra provision as developments take place and new ideas are tried. All students however, will have the opportunity to achieve a nationally recognised qualification.

2. ICT & Computing is taught and assessed through discrete ICT & Computing lessons timetabled in Key Stage 3 and Key Stage 4.

3. At Key Stage 5 students may opt for courses leading to more advanced ICT & Computing qualifications.

4. ICT is written into work schemes for all curriculum subjects and is used where appropriate to enhance and enrich the learning experiences of the students in those areas.

5. The procedures for assessing, recording and reporting will be carried out in accordance with the school's policy on assessment and reporting.

3. Whole School Policy

The effective use of ICT within the curriculum requires that pupils have appropriate access to a range of reliable and sustainable infrastructure of ICT services.

1. Equipment will be available to the students in a way that meets their learning needs.
2. A variety of strategies will be used, including single computers in classrooms, dedicated computer suites, wireless laptop networks, iPads and learning resources based in the Learning Resource Centre.
3. Equipment will be maintained and updated as required and as specified in the school's ICT improvement strategy.
4. There is a programme to ensure the replacement of obsolete computer equipment that does not wholly meet the requirements of the School Curriculum.
5. Maximum access to ICT resources will be achieved. This will link to any provision by the school of additional learning opportunities offered through out-of-school and cross-phase liaison.
6. 6. A clear set of policies governing the acceptable use of the ICT Network and the Internet are in place to protect staff, students and the system.

3.1 Curriculum delivery

1. The ICT & Computing Subject Leader is responsible for the teaching and learning in discrete ICT & Computing lessons at all Key Stages. Some of the responsibility for the running of particular courses may be delegated to other ICT specialists.
2. The Senior Leader with responsibility for ICT is responsible for overseeing and coordinating the development of teaching and learning across the curriculum.
3. It is expected that all departments will write into all schemes of work in all Key Stages appropriate elements of ICT.

3.2 Assessment, Recording and Reporting

The following strategies are in place:

1. The programmes of work identify clear opportunities for the monitoring and recording of the pupils' progress.
2. A clear recording mechanism.
3. Programmes of work include related tasks that assist the teacher to assess the pupils' ICT capabilities.

4. At Key Stage 3 ICT & Computing capability is to be assessed within discrete ICT & Computing lessons.
5. At Key Stage 4 ICT & Computing capability is to be assessed within specific ICT & Computing Courses that should all lead to a nationally recognised qualification.
6. Differentiated assessment for pupils with high levels of ICT capability, or special needs.
7. In line with whole school policy, progress and attainment in ICT & Computing will be reported as a separate subject at least once a year.
8. , Staff teaching subjects outside of ICT & Computing can find out the IT capability of individual pupils by accessing a copy of their projected grades which will be available in SISRA Analytics.

In the assessment spreadsheet they will be able to locate pupil levels and the names of the units undertaken. Further information on these units can also be found on the ICT section of PB iBook.

3.3 Staff Training

There are distinct areas for consideration:

1. Curriculum training.
2. Technical support and training for teachers.
3. Administrative user support.
4. Management of ICT within the classroom.

4. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Staff must ensure that they:

1. At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
2. Use personal data only on secured and encrypted, password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

3. Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

1. The data must be encrypted and password protected.

2. The device must be password protected (all staff have been provided with an encrypted USB stick.

3. The data must be securely deleted from the device once it has been transferred or its use is complete.

5. Learning Gateway

The school is mindful of the need for access to learning and data for staff, pupils and parents both during and outside of normal school hours. Therefore we have a learning and information system, called PB Gateway to facilitate this

The gateway is in operation and can be accessed both in and outside of school. It includes two very important components:

PB iCommunity, an information management console, which contains a range of useful and up-to-date information, proformas and active forms, which are used by members of staff.

In this section of the gateway staff can:

1. Access school documents, policies, current and past assessment data, behaviour proformas, finance proformas, PLT information, sixth form documents, student welfare information, and share resources.
2. Access room booking information and make requests.
3. Request ICT support though the HelpDesk form.

PB iBook, a Learning Gateway, which has been specially designed to support pupils, teachers and parents.

In this section of the gateway the user can:

1. Access course information
2. Access learning resources
3. Access past examination papers
4. Access extra-curricular information
5. Subject calendar information

iBook Subjects are amended and updated regularly.

The Gateway has improved the way in which we collect, store, exchange and manage data, enabling the easy movement of data between staff, pupils and parents.

The Gateway has been designed with care to take into consideration its usability by everyone, including visually impaired students and staff.

6. E-Mail

The purpose of this section of the policy is to ensure the proper use of the Microsoft 365 email system.

Plantsbrook School encourages staff and pupils to send emails instead of letters, faxes and other forms of paper communications where deemed appropriate. This form of contact provides quicker communication and is also a convenient way of filing such documents.

The email system should not be used as a means for sending unnecessary unsolicited emails, harassing groups or individuals or creating/continuing chain letters or spam. If an email is received or a student mentions an email that causes concern then a copy should be obtained where possible (either electronically or physically) and a member of the Senior Leadership Team should be informed. The matter will then be investigated and action taken as appropriate.

All emails should be read regularly, ideally once a day and archived for future reference (unless the content is unlikely to be needed in the future). A filing system in which to archive emails can be created. If you're unsure how to do this then please contact the - Learning Supporter through ICT.

All messages should have their content checked just as would be done for a physical document. Nothing should be sent in an email, especially to parents or contacts from outside of school that would not be appropriate in a letter.

Care should always be taken before opening attachments, especially if they are from someone that you do not know or were not expecting an attachment from. The school's network will do checking and filtering of viruses from attachments but it is not possible to catch 100% of problems. If you suspect that an email or attachment contains a virus or has caused a problem, inform the ICT support team.

Staff should only use the school approved, secure email account(s) for any school business. This could be by using the web based Microsoft 365 system or the Outlook/Outlook Express software. Web mail and hotmail accounts are not secure email system(s). Personal accounts should not be used for school business.

7. SIMS and SLG Usage Policy

This Policy applies wherever access to the Plantsbrook School SIMS management system interface is provided. This policy applies whenever information is accessed through the Plantsbrook school SIMS system, whether the computer equipment used is owned by Plantsbrook School or not.

7.1 Ownership and Administration of this Policy

Plantsbrook School owns and administers the policy.

7.2 Objectives of Plantsbrook School SIMS Usage Policy

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of Plantsbrook School's data, the authorised SIMS User and the individuals to which the SIMS data pertains. In particular these risks arise from:

- The intentional or unintentional disclosure of login credentials to the Plantsbrook school SIMS system by authorised users.
- The wrongful disclosure of private, sensitive, and confidential information;
- Exposure of Plantsbrook School to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This Policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy is adhered to.

This Policy aims to promote best use of the SIMS system to further the communication and freedom of information between Plantsbrook School and Parents\Guardians.

7.3 SIMS Usage Policy Rules

Authorised SIMS Users

- Plantsbrook School's SIMS system is provided for use by all members of staff.

7.4 Personal Use

Information made available through the SIMS system is confidential and protected by law under the Data Protection Act 1998. To that aim:

Users must not distribute or disclose any information obtained from the SIMS system to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility.

- Users should not attempt to access the SIMS system in any environment where the security of the information contained in the SIMS system may be placed at risk e.g. a cybercafé.

7.5 Password Policy

You must assume personal responsibility for your username and password. Never use anyone else's username or password.

You must always keep your individual user name and password confidential. These usernames and passwords should **never** be disclosed to anyone. Passwords and user names should never be shared.

In some instances users may be given the right to change the SIMS password from the one originally issued by the school. If this is the case the following rules must be followed:

- Passwords must be at least 6 characters (a-z, 0-9) in length
- Passwords must contain at least 1 number (0-9)
- Passwords must not be similar to your own name or username for example: cutler1

Questions, Complaints and Appeals

SIMS users should address any complaints and enquiries about the SIMS system to Plantsbrook School by email: enquiry@plantsbrookschool.co.uk or telephone: 0121 362 7310.

Plantsbrook School reserves the right to revoke or deny access to the SIMS system of any individual under the following circumstances:

- The validity of parental responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of the SIMS usage policy

If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

Please note: Where SIMS access is not available Plantsbrook School will still make information available according to Data Protection Act (1998) law.

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Any such misuse will be reported to the Headteacher and further actions may be taken as outlined in E-Safety Policy.

8. IT Disaster Recovery Plan

Disasters are difficult to predict, but by anticipating their effects and putting in place a carefully prepared Recovery Plan, the damage and disruption can be minimised.

This Plan describes the manner in which Plantsbrook School will respond to disasters affecting the IT systems, i.e. in the event of a complete network failure, power cut, server breakdown, fire or any other eventuality where the network is unavailable. This would include periods when the time taken to restore the network would take more than a day.

8.1 Risk Analysis

Risk	Probability	Impact	Plan
Virus	Medium probability	Variable impact	Sophos Anti-virus is being used across site and on staff laptops.
Fire	Low probability	High impact	There are existing school fire safety guidelines in place, please contact the site manager. A smoke alarm will be fitted before May 2016. Currently have smoke and gas/powder fire extinguishing.
Flood	Medium probability	High impact	The servers are situated in the main cabinet in the IT office, which gives some clearance for ground water.
Accidental Deletions	High probability	Low impact	Restoration from our current backups is very simple and fast. This process has been improved significantly in recent months. Test restores are carried out weekly to ensure that backups are good.

Theft	Low probability	High impact	A minimum of two but more likely three locked doors to break through to reach the server cupboard, plus there is an alarm.
Power Loss	High probability	Low impact	Uninterruptable power supplies are in place for the servers allowing them to shut down safely without risk of damage to data.

8.2 Server Backup and Restore

The department has a Disk to Disk to Tape backup system provisioned by RM and supplementary off site backups are made monthly.

Each server is backed up every weeknight, this backup includes the server operating system, configuration files and in the case of the Primary Domain Controller this would include network data such as usernames, policy and profile data and security information.

In the event of complete server operating system failure the server operating system would initially need to be re-installed then the server backup restored. In the event of server hardware failure, the server would first need to be repaired, then the server backup restored.

8.3 Data Restoration

Only the Network Manager and authorised personnel will have access to the means to restore network data. The Network Manager will determine if a successful restoration is possible.

Any requests for restoration of user data will be made to the Network Manager.
In the event of complete server failure where a full restoration of the school management software and data files is necessary, SIPS will need to be contacted.

8.4 Replacement of Supplies

It is the responsibility of the Senior Leader with responsibility for ICT to ensure that, as far as it is possible; the technical team have sufficient products and equipment for the discharge of their immediate service to the school. It is their responsibility, in the event of a disaster, to locate and where necessary replace all items that are either damaged, or lost.

8.5 Locations of Data

All critical data is backed up on-site and online. In the IT technician's office the servers are backed up to a tape drive and also to disk. SIMS data and data from the admin servers are backed up online every night.

8.6 Plan of Action

In the event of a large disaster involving server failure we will call SIPS for the admin domain and RM for the curriculum domain, to assist in the swift restoration of the backup data. This will allow the network to recover as quickly as possible, efficiently and without any extra problems associated with moving data around. Any extraneous data can easily be recovered by the on-site ICT Team from the backups and made available on a temporary network allowing certain staff to continue working while the process of recovery is underway.

9. Acceptable Use Policy

The computer systems within school are made available to students, staff, and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The School's Acceptable Use Policies have been drawn up to protect all parties - the students, the staff, other adults and the school and are reviewed on a regular basis. Staff and other adults wishing to use the School's computer systems, email or Internet should sign a copy of this Acceptable Use statement and return it to the Network Manager, James Merritt, for approval.

- All Internet activity should be appropriate to the students' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the School's ICT systems or activity that attacks or corrupts other systems is forbidden
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials and Intellectual Property laws must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail 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
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

If you access any site on the Internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the proforma to the Network Manager, James Merritt, unless it's a child protection issue where cases will be forwarded to Nicola Wigley or Lisa Proctor.

Misuse of the School's computer equipment, email or the Internet is a serious offence. The school reserves the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.