The Priory School

Whole School ICT Policy

Monitoring	Frame of engagement	Date
Member of Staff Responsible	Mr D Wright	September 2016
Governor Accountability	Full Governing Body	
Consultation Parameters	Unions SLT	
Information	Staff	
Date of latest version		2016
Date for next review **(and cycle)**		October 2018 Annual Review
Uploaded to Website		

The Priory School

Whole School ICT Policy

Statement of Intent

The Priory School's vision is that we will be a school where ICT is at the heart of innovative and enterprising learning and teaching. To enable this we must equip all learners with the experiences and skills within ICT that they will use in a rapidly changing technological world. Furthermore, we want our learners to be confident and independent in their use of ICT to solve problems across the curriculum.

The aims of this policy are to:

- meet the needs of the National Curriculum
- ensure that parents, staff, governors and the wider community have relevant and meaningful experiences of using ICT
- be as innovative and flexible in our use of resources as possible
- ensure the protection of confidentiality, integrity and availability of school information and assets.
- ensure users are aware of and fully comply with all relevant legislation.
- ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.
- ensure that staff and students are safeguarded when using ICT at The Priory School

The integrity of the Shropshire schools' network depends on the security policy implemented by each connected school.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The IT Network Manager is responsible for the school's ICT equipment, systems and data with direct control over these assets and their use, including responsibility for access control and protection. An employee of the school, the IT Network Manager will be the official point of contact for ICT or information security issues.

Procedures

- Users of the school's ICT systems and data must comply with the requirements of the appropriate Acceptable Use Policy / Contract

- Users are responsible for notifying the IT Network Manager of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Principal or Chair of Governors.

- If a member of staff should accidentally access inappropriate materials they should report it to their line manager or member of the Senior Leadership Team

- Deliberate access to inappropriate materials by a member of staff will result in appropriate disciplinary measures being taken.

- Users must comply with the requirements of the Data Protection Act 1998, Computer Misuse Act 1990 and Copyright, Designs and Patents Act 1988. Please refer to http://www.legislation.gov.uk/ for further guidance.

- Users will be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

- Users of the school's ICT systems and facilities will be provided with approved and authorised hardware and software to fulfil their designated roles. Any changes to environments are subject to prior approval of the IT Network Manager.

Information Security

- The School Business Manager has responsibility for whole school ICT infrastructure.

- Any data to be accessed from home is to be done by the Foldr website or App.

Physical Security

- Appropriate arrangements must be applied for the removal of any ICT equipment from its normal location. These arrangements should take into consideration the risks associated with the removal and the impact these risks might have.

- All school owned ICT equipment must be recorded and security-marked, subject to return conditions for leased equipment.

- An inventory of school hardware and software is maintained

- Staff must not leave sensitive or personal data on printers, computer monitors or desk whilst away from their desk or computer.

- Staff will not give out sensitive information unless the person is authorized to receive it.

- Staff will not send sensitive/personal information via e-mail or post without suitable security measures being applied.

- Staff will ensure sensitive data, both paper and electronic, is disposed of properly, e.g. shred paper copies and destroy disks.

System Security

- Users must not make, distribute or use unlicensed software or data

- Users must not make or send threatening, offensive or harassing electronic messages. Users should take time to consider the language and tone of any e-mail or messages sent to staff, students or any other stakeholder.

- Users must not create, possess or distribute obscene material

- Users must ensure they have authorization for private use of the school's computer facilities

Personal computer equipment, including portable storage devices, should not be used on the school's computer system without the prior authority of the IT Network Manager for staff or a member of staff for students.

- The IT Network Manager will determine the level of password control

- Passwords must be memorised

- Passwords should not be revealed to unauthorised persons

- Passwords should not be obvious or guessable and their complexity should reflect the value and sensitivity of the systems and data

- Passwords must be changed if affected by a suspected or actual breach of security, eg when a password may be known by an unauthorized person

- Regular backups of data, in accordance with the recommended backup strategy, must be maintained.

- Security copies should be regularly tested to ensure they enable data restoration in the case of system failure

- Where possible, security copies should be clearly marked and stored in a fireproof location and/or off site.

Virus Protection

- The IT Network Manager will ensure current and up to date anti virus (AV) software is applied to all school ICT systems

- The IT Network Manager will ensure operating systems are updated with critical security patches as soon as these are available.

- The IT Network Manager will ensure users of home/school laptops check for critical security patches/AV updates when connecting laptops to the school network.

- Any suspected or actual virus infection must be reported immediately to the IT Network Manager

Disposal and Repair of Equipment

- The IT Network Manager must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.

- It is important to ensure that any software remaining on a PC being relinquished is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.

- The IT Network Manager must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

- The school will ensure that third parties are registered under the Data Protection Act as personnel authorised to see data and as such are bound by the same rules as school staff in relation to not divulging the data or making any unauthorised use of it.

The use of handheld technology (including mobile phones and iPads)

In line with our aim of being as innovative and flexible in our use of resources as possible the school recognises that handheld technology and mobile phones present many opportunities for innovative and enterprising learning and teaching. To this end the following policy applies:

Cyberbullying

- Staff and students will be vigilant with regard to the use of ICT as a method and mode of bullying. This will be addressed using the school's Behaviour policy, even if it occurs via social media outside of school hours.
- Specific anti-cyberbullying talks and events will be arranged within Life and promoted by all staff.
- Groups and individuals who are both victims and perpetrators will be supported by the schools pastoral and support teams.
- Where it becomes a hate crime, police intervention and involvement will occur.
- All curriculum areas, not just Computing/ICT, have a responsibility to promote positive use of social media and discourage cyberbullying.

Students are permitted to bring a mobile phone to school. Generally mobile phones:

1. Must be kept in the students' bags and switched off
2. Are not the responsibility of the school in terms of loss or damage
3. Where the mobile phone has the capacity to take photos or video clips students are expressly forbidden from using these facilities unless their teacher has directed them to.

However, there are many opportunities presented by modern mobile technology. Staff are actively encouraged to make the most of these opportunities as they present themselves.

Students are permitted to use iPads in school where this is part of the learning and teaching activity within a lesson or part of their general studies eg. homework. Any iPad used within school should either be part of the school's leasing system (and therefore meets the password and data protection criteria) or have been verified by the schools IT Network Manager prior to use.

- All students must have signed the iPad acceptable use agreement.
- School sanctions will be used to address any misuse, in line with the school behaviour policy
- Staff should also sign and agree to an iPad acceptable use policy for their school iPad and use it according to these purposes.

Data Sticks

In line with the school's aim for home access to be flexible in its use of technology we accept that data sticks may well be necessary. However, please ensure that these are encrypted as not to break Data Protection Laws if they carry student data. Therefore students may only upload data from a memory stick with the express permission of the IT Network Manager. All memory sticks will be scanned for viruses and any programme will be quarantined if deemed to be dangerous to the network.

Acceptable Use Policy / Agreement

The school believes that any communications technology should be used without creating unnecessary risk to users while supporting learning. To this end users of ICT at the Priory will need to sign the appropriate Acceptable Use Agreement as outlined below:

The Priory School ICT Acceptable Use Agreement (Students)

Students should make themselves familiar with the Network and BYOD Agreements in their welcome pack. Extra copies are available upon request.

When I am using a computer or other technologies, I want to feel safe.

I agree that whilst in school I will:

- Always keep my passwords a secret
- Only visit sites which are appropriate to my work at the time (i.e. not chat sites or social networking sites)
- Work in collaboration only with friends and I will deny access to others
- Tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
- Make sure all messages I send are respectful
- Show a responsible adult if I receive an offensive or unsettling message receive anything that makes me feel uncomfortable
- Not reply to any offensive or unsettling message or anything which makes me feel uncomfortable
- Not give my mobile phone number to anyone who is not a friend
- Only email people I know or those approved by a responsible adult
- Only use email which has been provided by school
- Always keep my personal details private. (My name, family information, journey to school, my pets and hobbies are all examples of personal details)

- Always check with a responsible adult and/or my parents before I show photographs of myself
- Use my iPad according to the iPad acceptable use agreement

I know that once I post a message or an item on the internet then it is completely out of my control.

I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

I agree that I will not:

- Visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornography
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Radicalisation and Extremism
    - Promoting illegal acts
    - Forward chain letters
    - Breach copyright law
    - Do anything which exposes other children to danger

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used for a variety of purposes.

Signed: _____ Date: _____

Print name: _____

The Priory School ICT Acceptable Use Agreement (Staff)

Staff should make themselves familiar with the laptop/iPad agreement they have signed which outlines their responsibilities in respect of the physical security of their laptop and the data on it.

I agree that I will:

- Only use personal data securely
- Implement the school's policy on the use of technology and the digital literacy of students
- Use opportunities to educate students in the effective use of the internet in research, including the skills of knowledge, location, retrieval and evaluation
- Use opportunities to educate students in the recognition of bias, unreliability and validity of sources
- Use opportunities to actively educate learners to respect copyright law
- Only use approved e-mail accounts
- Only use student images or work when approved by parents
- Only give access to appropriate users when working with blogs or wikis
- Report unsuitable content or activities to the IT Network Manager.
- Ensure that videoconferencing is supervised appropriately for the learner's age
- Pass on any examples of internet misuse to a senior member of staff
- Use my school iPad according to the acceptable use policy
- IPads and laptops should be left in the UK securely when travelling abroad.
- Adhere to the Staff Code of Conduct

I agree that I will not:

- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornography
    - Promoting discrimination of any kind
    - Promoting racial or religious hatred
    - Radicalisation and Extremism
    - Promoting illegal acts
    - Breach any LA / School policies (e.g. gambling)
    - Do anything which exposes children in my care to danger
    - Any other information which may be offensive to colleagues

- Forward chain letters
- Breach copyright law
- Do anything that puts a young person at risk
- Make or send threatening, offensive or harassing electronic messages. Users should take time to consider the language and tone of any e-mail or messages sent to staff, students or any other stakeholder.

I accept that my use of school and LA ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed: _____ Date: _____

Print name: _____