ST IVO SCHOOL

Whole School ICT Policy

Incorporating E-Safety, Social Media, Use of Student Photos/Videos and Acceptable Use Policies

Approved: December 2016, Full Governing Body

Updated for GDPR Compliance: May 2018

Next review due: December 2018

The key aim of the whole school ICT team is to support stakeholders in using ICT as an effective tool for learning, teaching, communication, management and administration, whilst prioritising e-safety issues.

1. Whole school use of ICT
   - 1.1. All students and staff are issued with individual school network and email accounts, both with individual usernames and passwords.
   - 1.2. The school looks to use ICT systems as far as possible to enhance learning and/or enable increased efficiency, effectiveness, monitoring and communication. For example:
     - 1.2.1. Go4schools, an online system accessible from inside and outside school, is used by teachers for recording targets, assessment results, reports, attendance, homework tasks and behaviour. Parents and students also have access to this system.
     - 1.2.2. ParentMail is used to send letters home to parents/carers, and for parents/carers to make payments to the school, including for trips, uniform and cashless catering topups.
     - 1.2.3. Foldr can be used by students and staff to access network files from outside school.
   - 1.3. The school website and social media accounts are used to support communication with parents/carers and other interested parties. Several departments, areas and individuals have their own social media accounts. A protocol is in place to guide staff use of social media accounts, staff must discuss the creation of any new accounts with the Director of School Strategic Operations who will issue them with the protocol.
   - 1.4. The school has the right to use photos and or video as part of internal systems for teaching, learning and administration. Parents and students receive a copy of Appendix A requesting consent to use photos/videos in other ways for celebrating success, promoting events and marketing.

2. Access to whole school resources (in particular ICT Suites)
   - 2.1. Students have access to a variety of ICT facilities. The majority of ICT suites are available to be booked by other departments using an online booking system once Computing Department lessons have been timetabled.
   - 2.2. Some departments have exclusive use of an ICT suite, clusters of computers and/or mobile devices for student use, for example PE and D&T.
   - 2.3. Computers are also available for booking in the Resource Centre.
   - 2.4. Sixth Form students have exclusive access to computers in Sixth Form study areas.
   - 2.5. There is wireless access throughout the school, for the use of staff, adult education classes and students in Year 8 and above. Visitors may also be given access at the discretion of the ICT Technical Manager. There is a secure wireless network for school owned devices, and a “guest” network for personal devices.
   - 2.6. All classrooms have a computer, speakers, projector and interactive whiteboard.

2.7. All teaching staff on permanent contracts are provided with a school iPad, those on fixed term or temporary contracts may be provided with an iPad at the discretion of the Director of School Strategic Operations.

2.8. Microsoft Office is installed on all computers. Departments are free to purchase software, however budget holders have a responsibility to ensure that software is appropriately licensed before installation. This is overseen by the ICT Technical Manager.

2.9. Computers are replaced on a rolling cycle, budget permitting. Many computers in the school have an expected life span of 6 years, with possible redeployment to less critical areas in this time. Equipment being disposed of is collected by a recycling company who guarantee data destruction. Replacement of equipment used solely by one subject is the responsibility of that department.

2.10. A full backup regime is in place for the school's servers and file storage devices. Incremental backups are taken every week night. All backups are encrypted and stored in a secure location in a separate building to the main servers.

3. E-Safety

3.1. The school has Acceptable Use Policies in place for students (Appendix B) and staff (Appendix C).. There is an additional Acceptable Use Policy for those staff with school iPads (Appendix D). All staff and students are reminded of the Acceptable Use Policies at the start of each academic year.

3.2. E-safety is covered in Computing lessons for Years 7 to 9 at the start of every academic year, and reinforced through assemblies led by the Assistant Head with responsibility for whole school ICT.

3.3. All internet access in school is filtered by Lightspeed Systems content filter, purchased through Cambridgeshire County Council ICT Service with different levels of filtering for Years 7 to 11, Sixth Form and staff. Users accessing the internet using a mobile device must authenticate to the system every day using their network username and password. The same level of filtering applies across the wireless and wired networks. Management of content filter settings is the responsibility of the ICT Technical Manager, with certain categories being blocked at County level.

3.4. School leaders are experienced in dealing with e-safety issues. Student related matters are generally dealt with by pastoral leaders or the Inclusion Manager, supported by senior leaders and/or the ICT Technical Manager as appropriate. Issues that arise regarding staff e-safety are addressed by the Headteacher, a Deputy Head, the Assistant Head with responsibility for whole school ICT or the Director of School Strategic Operations. Any potential staff disciplinary matters will be dealt with by the Headteacher or a Deputy Head supported where appropriate by the Director of School Strategic Operations and / or the Assistant Head with responsibility for whole school ICT. An exemption agreement, authorised by the Personnel Committee of the Governing Body as a staffing matter, exists to allow certain staff the use of a personal device for photographing and videoing students, this agreement is issued to named staff at the discretion of the Headteacher and Director of School Strategic Operations. Please also refer to the school's Data Policy for information regarding secure access to and transport of data.

ST IVO SCHOOL – WHOLE SCHOOL ICT POLICY – APPENDIX A

Use of Photographs and Videos of Students

St Ivo School recognises both the benefits and risks pertaining to the use of photographs and videos which include students. Whilst these can act as an encouragement to students, a way to celebrate success, remember an event, a marketing tool etc, the school takes the issue of child safety very seriously, and understands that use of photos/videos containing their child(ren) may be a particular issue to some families due to individual circumstances in this "digital age".

On arrival at the school and when this policy is reviewed, parents/carers will be sent a copy of this document to request their consent.

School use of student images and video

The school requests consent from parents/carers for their child to be photographed and/or filmed, and for this media to be used in the following ways:

- In St Ivo publications
- On the St Ivo website and official, whole school social media accounts including Facebook, Instagram, Twitter and YouTube (full names of students will not be publicly available alongside photographs, except where permission has been obtained from parents/carers at the time of publication)
- On other social media accounts controlled by a school employee and not openly accessible (for example, as part of a Twitter feed where tweets are marked as private but students and parents/carers can ask to "follow" the account, or as part of a video of a school event placed on YouTube but not in public listings).
- By the local press (full names of students will not be publicly available alongside photographs, except where permission has been obtained from parents/carers)

If parents/carers give consent, this can be withdrawn at any time by writing to the school or by email to award@stivoschool.org. Our records will then be updated accordingly for all future use. Under data protection law, this right transfers to the child at age 13.

In all cases, the school retains the right to use photographs and videos of students for internal systems which are only accessible to school employees.

Parents/Carers taking photographs at school events

Whilst we understand that parents/carers may wish to take photographs and/or video recordings at school events, in the interests of the safety of every child present no photography or filming by parents/carers is allowed at events which take place on school site (including school events taking place at One Leisure facilities). Some productions and shows at the school have an official photographer and/or a member of staff taking photos or videoing the event. In certain circumstances and dependent on the children in attendance, the member of staff in charge of the event may grant permission for parents/carers to take photographs.

In the interests of child safety, we would ask that parents/carers do not place any photographs/video including St Ivo student other than their own child(ren) on publicly accessible websites and social media.

ST IVO SCHOOL – WHOLE SCHOOL ICT POLICY – APPENDIX B

Student Use of ICT - Acceptable Use Policy

As part of your learning experience at St Ivo School you will use the internet and other ICT resources to help you with your work. It is important that you stick to the following rules to make sure you use the internet and ICT resources safely and appropriately.

1. At St Ivo School, we expect you to be responsible for your own behaviour on the internet and when using ICT facilities, just as you are anywhere else in school. This includes materials and websites you choose to access, the language you use and using safe practices such as not telling anyone else your login password. Please note use of ICT facilities provided by school is monitored.

2. When using the internet make sure you only go to suitable, educational sites. If you find any unsuitable sites you must report it immediately to your teacher.

3. Be careful in the language you use, particularly in email communications and only contact people you know or those the teacher has approved. You must not get involved in sending chain letters and only visit chat rooms when given permission to do so by your teacher, in which case the teacher will monitor use of the chat room.

4. Your parents/carers may choose to allow you to use social networking sites (for example Facebook, Instagram and Snapchat) at home, however on the school network and wifi the use of these is not permitted. Any occurrence of cyber-bullying using social media that impacts on those in school or other ICT methods such as texting will be dealt with severely. You must use caution when posting information online including on social networking sites and blogs; you must not post material which could damage the reputation of yourself, other people or the school.

5. You must not use your mobile phone during lesson time, including on your way to lessons, without the permission of a member of staff.

6. Photos and videos must not be taken on the school site, during school trips or any other school activity without the permission of a member of staff.

7. You must not download files to the computer or network from the internet without permission (they may contain viruses or damage the school network). In addition any attempt to bypass school security, such as hacking the network, will be treated as a suspendable offence.

8. It is vital that network security is not compromised. Removable media can be bought into school, however these should be used with caution as they may include viruses or other malicious software. The ICT Manager has the right to confiscate any such media if it is believed that network security may be compromised.

9. It is important that personal information such as full names, telephone numbers and addresses (including email addresses) should not be given out and you must not arrange to meet someone unless this is part of an approved school project.

10. If you choose not to follow these expectations, you will be warned and subsequently, may be denied access to ICT resources, or face further sanctions.

ST IVO SCHOOL – WHOLE SCHOOL ICT POLICY – APPENDIX C

Staff Use of ICT - Acceptable Use Policy

St Ivo School seeks to embrace the use of ICT to enhance teaching and learning in the school. This guidance on appropriate use of ICT has been put together to fulfill government requirements, and should be read in conjunction with the Acceptable Use Policy for Data. All staff with access to the ICT network are required to agree to it.

Use of the Internet

1. All use of the internet at school should be primarily to enhance teaching and learning or for administrative use.
2. It is understood however that staff may occasionally need to use the internet for personal reasons. Such use should be limited to outside of lesson time for teaching staff and during breaks/lunchtimes for support staff.
3. Internet access in school can be monitored. Appropriate filtering systems are in operation for both staff and students.
4. The accessing of inappropriate or indecent materials from the internet or via e-mail will be investigated, which may result in disciplinary action being taken.

Social media

1. Staff must use caution when posting information online including on social networking sites and blogs. Staff must not post material which could be seen as damaging to the reputation of the school or cause concern about their suitability to work with students. Staff posting material which could be considered inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
2. Staff must not be “friends” with or “follow” students on any social network websites, with the sole exception of family members. Staff are strongly advised to set accounts to “private”.
3. Staff who manage social media accounts for their department, area or which are otherwise associated with the school must follow the social media protocol. In particular, the creation of accounts must be authorised by the Director of School Strategic Operations, accounts (except the whole school accounts) must be “private” if you wish to post photos and videos of students and you must give due regard to the list of students who whom photo consent has been withdrawn.

Use of E-mail

1. All staff have a school e-mail address. Use of this e-mail address is encouraged for correspondence with the school and externally as required. Staff must use this school e-mail address to communicate with students, and not personal addresses.
2. Email should be treated as inherently insecure. You need to be careful of the language you use in all correspondence. Please be considerate with numbers of emails sent, ensuring that all methods of online communication (e.g. daily bulletins) are used appropriately. A separate communication protocol exists which you should follow. Email communications may be required to be made visible to parents/carers or students under the General Data Protection Regulation, so always bear this in mind when writing about students. Refer to the school’s Data Policy for further information.

Use of the ICT network

1. Each member of staff has a unique login for the network. It is strongly recommended that you change your password for network access regularly (at least once a term). Passwords should not be obvious, and ideally include alpha and numeric characters and a mix of upper and lower case. Passwords should never be divulged to other staff and especially students. Accounts will lockout after five incorrect password attempts.

2. When using an ICT suite with students, you understand that you are expected to be in the room at all times and are responsible for ensuring that use of the facilities by students is appropriate. You may be held responsible for any damage that occurs whilst your class is in the ICT suite.
3. It is the responsibility of all staff to ensure that students do not have access to confidential data including go4schools and SIMS. You must therefore be vigilant in their security measures e.g. locking out your computer when leaving the room for a short period of time.
4. Data stored on the network is backed up regularly; staff should however ensure that data on removable media and laptops is also backed up.
5. Please note that your network activity (including home area) can be monitored.
6. It is vital that network security is not compromised. Removable media can be bought into school, however these should be used with caution as they may include viruses or other malicious software. The ICT Manager has the right to confiscate any such media if he believes that network security may be compromised.
7. Staff may connect personal devices to the "ivo_guest" wireless network. Departmental purchases of new ICT hardware should be approved by the ICT Technical Manager.
8. Software loaded on school owned devices must be appropriately licensed. Budget holders have a responsibility to ensure that software purchased is licensed appropriately. Software installations on networked PCs should be approved by the ICT Technical Manager.
9. Equipment may be taken home at the discretion of the line manager/Head of Department.

E-safety

1. Whilst access to unsuitable internet content is minimised by filtering software, this can never be completely eliminated. It is therefore important that staff recognize their duty of care to ensure that students do not access or search for inappropriate website content. In addition students should not give out personal information online (including through e-mail).
2. For reasons of child and data protection, identifiable student data should not be stored on personal devices or online with the exception of school approved systems such as Go4Schools, Doddle, etc.
3. Staff accessing inappropriate material or using ICT facilities irresponsibly will be treated seriously. Disciplinary action and police involvement may result.
4. If you suspect that illegal content has been accessed on a computer, the workstation should be immediately powered down (pull the power cable) and secured. Do not attempt to check whether content is illegal by accessing it and contact a member of the Senior Leadership Team immediately.

If you have any questions or concerns regarding the above, please contact the Director of School Strategic Operations or Assistant Headteacher with responsibility for whole school ICT.

Staff name _____

Signature _____ Date _____/_____/_____

ST IVO SCHOOL – WHOLE SCHOOL ICT POLICY – APPENDIX D

iPads – Acceptable Use Policy

This agreement lays out the conditions for staff use of iPads (iPods and other tablets) at St Ivo School. This agreement supersedes any previous agreements.

1. You are responsible for ensuring the physical security of the iPad. You should set a passcode on the iPad, and set it to wipe all data if the passcode is entered incorrectly 10 times, and must install the school's management profile on the iPad. Store the iPad out of sight – e.g. do not leave it in view in an unattended car.

2. You may take the iPad out of school, but are expected to have it in school every day for use as a teaching tool. When using the iPad out of school, ensure that your use is appropriate for an educational setting – remember that the iPad will store your internet history etc which may be accidentally viewed by students.

3. You may install apps on the iPad, both for educational and personal use. The latter must again be appropriate to be viewed in an educational setting. The iPad must not be "jail broken". You should ensure that you check for updates to the iPad and apply these on at least a monthly basis.

4. You may store data (documents, photos, videos etc) on the iPad, as long as this is consistent with the school's Data Protection Policy, legal and appropriate for use in an educational setting. In particular, you must not store student data containing two or more pieces of identifiable information on the iPad e.g. name and date of birth. Contravention of this may result in disciplinary action.

5. The school provides wireless access for mobile devices in most parts of school site. You are responsible for the cost of internet access outside of school. You can access your network home area and Projects through the school's Foldr service.

6. Should any faults or damage occur, inform the ICT Technical Manager as soon as possible. Facts will need to be discussed and agreement reached on funding for repairs/replacement. Any repairs should be arranged with Apple after you have informed the ICT Technical Manager.

7. If your iPad goes missing or is stolen, the Director of School Strategic Operations must be informed as soon as possible. In the event of an insurance claim, facts will need to be discussed with the school and agreement reached on responsibility for payment of the insurance excess.

8. Government and school policies regarding appropriate use, data protection, computer misuse and health and safety must be respected and promoted by all staff, at school and at home. Please ensure you have read the whole school ICT policy and understand the meaning of 'appropriate use'.

Staff name _____

Signature _____ **Date** _____/_____/_____