STUDLEY HIGH SCHOOL
AN ACADEMY TRUST SCHOOL – ALWAYS AIMING HIGHER

ICT Policy

Review Period: Annually

Review By: Leadership Group & C&C

Contents:

Introduction
The key aim of the whole school ICT team is to support stakeholders in using ICT as an effective tool for learning, teaching, management and administration, whilst prioritising e-safety issues. It is our vision that ICT is fully exploited in all curriculum areas within the school to broaden the curriculum and learning opportunities for all pupils. In turn this will build learners e-confidence and develop a community of respectful digital citizens.

1. Whole School

1.1 All students and staff are issued with individual school network accounts

1.2 The school looks to use ICT systems as far as possible to enhance learning and/or enable efficiency, effectiveness and monitoring. For example:

- 1.2.1 Sims is used by teachers to record targets, assessment results, reports, attendance and behaviour.
- 1.2.2 Groupcall is used to send letters home to parents/carers, and Parentpay enables parents/carers to make payments to the school, including, but not limited to: payments for trips, revision guides and cashless catering top ups.
- 1.2.3 Real Smart can be used by students and staff to access and save files from anywhere, set and mark homework activities and share resources.
- 1.2.4 Classcharts, to track behaviour & seating plans
- 1.2.5 Cunninghams Biostore for Cashless canteen purchasing
- 1.2.6 Exam boards eg AQA, Pearsons, EdExcel, WJEC
- 1.2.7 Medical Tracker for first aid monitoring
- 1.2.8 Groupcall for group text messaging
- 1.2.9 Papercut for print solution monitoring
- 1.2.10 Exeant Trip Management
- 1.2.11 Library monitoring software
- 1.2.12 ACE for attendance monitoring and reporting
- 1.2.13 SISRA for statistical review monitoring
- 1.2.14 Various departmental online homework app's enabling pupils to complete revision and homework online

1.3 The school website and school social media accounts are used to support communication with parents/carers and other interested parties. Many departments have their own Twitter feeds.

1.4 All parents have received a letter stating the ways in which we may use photos/videos of their child. Parents can withdraw permission for photographs to be used on the website and in media if they wish.

2. Resources

2.1 Access to ICT suites is prioritised as follows:

- 2.1.1 Core Computing lessons are timetabled and roomed on to the main school timetable
- 2.1.2 Bookings for departments with particular requirements for ICT access in order to complete the course are then timetabled
- 2.1.3 Departments are able to book free ICT rooms (I1, I2 or library) by seeing KG

2.2 Some departments have clusters of computers and/or laptops for student use

2.3 There is a secure wireless access throughout the school, for the use of staff

2.4 All classrooms have a computer/laptop/tablet, speakers, projector and screen

2.5 Microsoft Office is installed on all computers. Before software is purchased by individual departments it must be tested for compatibility by the IT team. For subject specific software it is the responsibility of the budget holder to ensure that software is appropriately licensed. This is overseen by the Director of IT

2.6 Computers are replaced as necessary, budget permitting

2.7 A full backup regime is in place for the schools servers. During term time, a daily backup is taken and every 4 weeks a long term backup is taken and retained for a period of 6 months. All backups are stored in a secure location either on site servers or backed up to Azure in Microsoft's Data Centre facilities within the European Economic Area (EEA)

2.8 IT services will provide all technical support via the "helpdesk". All requests for support should be directed to the helpdesk. If an issue is urgent IT support can be contacted internally by phone and followed up at a convenient time through the helpdesk

3. E-Safety

3.1 The school has acceptable use Policies in place for students and staff, which are shown on the following pages. 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 year 7-9, at the start of every academic year, and reinforced through whole school assemblies. E-safety is an integral part of Personal Development days in all year groups.

3.3 Staff, parents/carers and friends of the school are invited to separate training sessions which run on an annual basis.

3.4 All Internet access in school is filtered by Light Speed content filter with different levels of access for staff and pupils.

4. Curriculum

4.1 ICT is embedded within the framework of the planning and delivery of all subjects taught within the school. It is incorporated in the planning for each scheme of work and students will be able to develop ICT skills, not only through their Computing lessons but also through cross-curricular work.

4.2 Through the use of our integrated ICT system (e.g. Real Smart) we will endeavour to deliver:

4.2.1 Extended learning resources

4.2.2 More flexible study – providing a choice of where, when and how students study

4.2.3 Individual e-mail access for staff and students

4.2.4 Unlimited cloud based storage space

Student Use of ICT – Acceptable Use Policy

At Studley High 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 web sites you choose to access, the language you use and using safe practices.

(Pupil speak)

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

I agree that I will:

1. Always keep my passwords a secret
2. Only visit sites which are appropriate to my work at the time
3. Work in collaboration only with friends and I deny access to others
4. Tell a responsible adult straight away if anything makes me feel scared or uncomfortable online
5. Make sure all messages I send are respectful
6. Show a responsible adult if I get a nasty message or get sent anything that makes me feel uncomfortable
7. Not give my mobile number to anyone who is not a friend in real life
8. Only email people I know or those approved by a responsible adult
9. Only use email which has been approved by school
10. Talk to a responsible adult before joining chat rooms or networking sites
11. Always keep my personal details private (My name, family information, journey to school, my pets and hobbies are all examples of personal details)
12. Always check with a responsible adult and my parents before I show photographs of myself
13. Never meet an online friend without taking a responsible adult that I know with me

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 website that I visit may be viewed by a responsible adult

Staff Use of ICT – Acceptable Use Policy

Studley High School seeks to embrace the use of ICT to enhance teaching and learning in the school.

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 pupils
4. The accessing of inappropriate or indecent materials from the Internet or via e-mail may result in disciplinary action being taken
5. Staff must use caution when posting information online including on social networking sites and blogs. Staff must not post material damaging the reputation of the school or which could 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
6. Staff must not be "friends" with students on social network websites, and are strongly advised to set accounts to "private"

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 (if necessary) and not personal addresses
2. There is an expectation that all staff check e-mails on a daily basis (Monday – Friday during term time)
3. Email should be treated as inherently insecure. You need to be careful of the language you use in all correspondence. Please be considerate of the numbers of emails sent, ensuring that all methods of communication (e.g. daily bulletin) are used appropriately

Use of 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 pupils.
2. When using an ICT room with pupils you are expected to be in the room at all times and are responsible for ensuring that use of the facilities by pupils is appropriate.
3. It is the responsibility of all staff to ensure that that pupils do not have access to confidential data including Sims. You must therefore be vigilant in their security measures e.g. Locking out your computer when leaving a room, not storing sensitive information on removable media
4. Data stored on the network in backed up regularly; staff should however ensure that data stored on removable media and laptops is also backed up
5. Please note your network activity (including home area) can be monitored
6. It is vital that network security is not compromised. Removable media can be bought in to school, however these should be given to the IT Network Manager for encryption and password protecting. They should be used with caution as they may include viruses or malicious software
7. Only school related documents may be stored on the school network
8. Staff may connect encrypted personal devices to the wireless network. Departmental purchases of new ICT hardware should be checked for compatibility and approved before it is ordered
9. Software loaded on school owned devices must be appropriately licensed
10. Equipment may be taken home but is expected to be brought back into school every day to be used as a teaching tool as appropriate

E-Safety

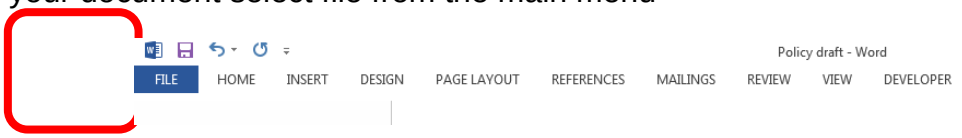
1. Whilst access to unsuitable internet content in minimised by filtering software, this can never be completely eliminated. It is therefore important that staff recognise their duty of care to ensure that pupils do not access or search for inappropriate website content. In addition pupils should not give out personal information online (including through e-mail)
2. For reasons of child protection, pupil data and photographs should not be stored online unless in a secure area
3. Staff accessing inappropriate material of using ICT facilities irresponsibly will be treated seriously. Disciplinary action and police involvement may result

Data Protection

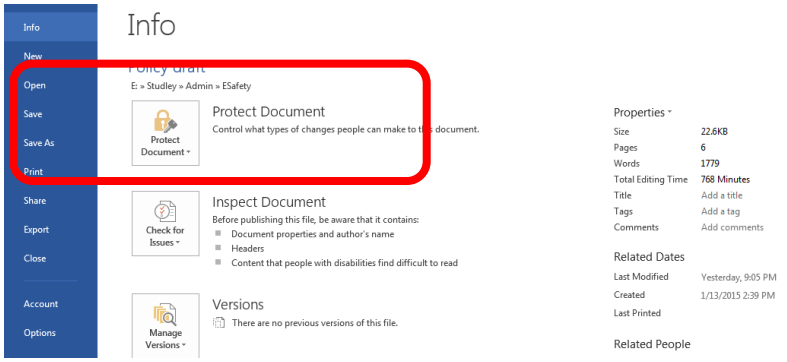
1. To ensure compliance with the Data Protection Act it is recommended that pupil data is not stored on unencrypted portable or external devices, such as memory sticks, flash drives, CDs or external hard drives
2. Student data such as full names, addresses, ethnic origin, socio-economic status, etc. should NEVER be stored on personal devices
3. Any document containing pupil data that is stored on a portable device including laptops/tablets must be password protected. (See Encrypting a Document Help below)

Encrypting a Document Help Sheet

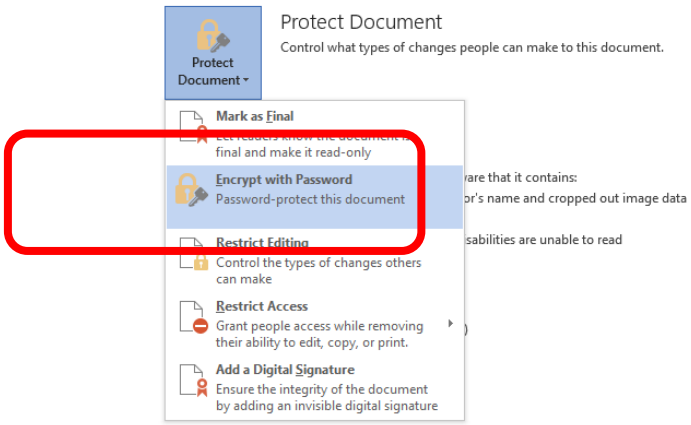
1. In your document select file from the main menu



2. Select protect document



3. Select encrypt with password



4. Enter a password

PLEASE BE AWARE THAT IF THE PASSWORD IS FORGOTTON IT CANNOT BE RECOVERED!