ICT AND E-SAFETY POLICY

Including:
Laptop and Mobile Device Policy.
E-safety and Cyberbullying Policy.
Social Networking Policy

Date Published:	**March 2017**
Version:	**V3**
Authors:	**A.Fell**
Date shared with Governors:	**March 2017**
Review Date:	**JANUARY 2018**
Date shared with Staff:	**March 2017**

ICT CURRICULUM USAGE AND NETWORKING POLICY

PURPOSE AND AIMS

ICT plays a vital part in our lives and it is constantly changing, requiring us to learn and encompass more and more technological information. It provides a powerful communication tool, allowing us to analyse and respond to a wide range of information. It is also recognised as a strong motivating force for children to support the raising of standards across all curriculum areas.

AIMS

- To provided access to ICT opportunities for all children and staff
- To ensure ICT is used across the curriculum and in the wider work of the school
- To monitor, record and assess children's progress across the curriculum
- To promote safe and responsible use of ICT
- To develop the profile of the school through the school's website
- To keep pace with developing technology

ROLES AND RESPONSIBILITIES

The ICT technician is responsible for

- Ensuring all hardware and software is working ready for use as far as is possible
- Being available for troubleshooting with IT issues
- Advising on purchasing hardware and all software for academy
- Purchasing curriculum software
- Tracking use of curriculum software
- Ensuring the website is kept up to date and compliant with Ofsted
- Backing up data
- Ensuring web filtering and security maintains the integrity of safeguarding

The ICT Co-ordinator is responsible for:

- Ensuring that policy is best practice, up to date and fit for purpose through monitoring of the policy, its review and update annually.
- Monitoring children's progress within the computing curriculum
- Monitoring the effectiveness and impact of ICT on outcomes and the personal development and well-being of staff and students.
- E-safety committee (as part of H&S, Wellbeing Committee)
- Develop an e-safety culture, act as a named point of contact on all e-safety and promote the e-safety vision to all stakeholders and supporting them in their understanding of the issues
- Ensure that e-safety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that e-safety is embedded across the curriculum and activities within the organisation as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the trust and other local bodies as appropriate

Staff are responsible for

- Reporting any ICT issues to the ICT technician.
- Ensuring E-safety is of the highest priority.
- Providing high quality integrated computing and ICT learning opportunities for children to apply skills cross curricular subjects
- Planning skills based plans for progression
- Fully complying with this policy
- Ensure that they understand the risks that the students face
- In the event of a disclosure report it using the school's Child Protection and Safeguarding Policy
- Supervision of students at all times when using ICT

The Principal/Head of School is responsible for:

- Ensuring appropriate arrangements are in place to comply with this policy
- Making sure all users are aware of this policy
- Ensuring that appropriate training is undertaken
- Ensuring that the technical infrastructure / network is as safe and secure as possible
- Updating the list of inappropriate websites which fall through the filtering software
- Investigation and implementation of discipline matters in relation to this policy.

Governors through the Health, Safety and Well-being committee are responsible for:

- Appropriate budget is allocated to enable the academy to maintain and develop further ICT capability.
- Overseeing the implementation of the ICT policy
- Undertaking the role of the E-safety work group in partnership with the Whizz Kids and parents as appropriate.

CURRICULUM

All children will be given opportunities to:

- develop word processing skills
- develop control of wide range of hardware including tablets, laptops and PCs.
- develop Computer Aided Design skills
- use a range of multimedia software across the curriculum
- use ICT to communicate with others
- simulate and model situations
- store, retrieve and communicate data
- use ICT to create music
- research and find out information
- develop coding and programming
- learn how to be safe online and how to prevent and deal with cyber-bullying

- learn how to ensure that they work safely on ICT equipment e.g. posture and length of time with regards eye-strain.
- incorporate appropriate terminology in their work as well as make good use of ICT learning across the curriculum.
- Manage their own file directories

1. ICT is integrated across the curriculum, to support outstanding teaching, learning and assessment.

2. All staff and children have access to the filtered internet including the use of e-mail as a key communication tool

3. Children are given opportunities to use a range of technology including tablets, data loggers, raspberry pi laptops including Roamers, Beebots, ipads, digital cameras, microphones etc

4. Staff will use ICT in order to inform and enhance their own professional practice.

5. Resources including hardware will be managed and future development will be planned for.

6. Parents/guardians will be asked to sign a consent form for use of images.

7. All students will be asked to complete an Acceptable Use of the Internet form list of children without consent is kept in each classroom and centrally by the admin team.

STAFF COMPUTER SECURITY AND PROTECTION

Each member of staff will be provided with an encrypted personal account for accessing the computer system, with their own username and password. This account will be tailored to the level of access required and will be for that user's use only. As such, users must not disclose password information to anyone, including the ICT Technicians. In the event of a password becoming compromised, users will be required to change their password immediately.

- Passwords will be updated as per protocols decided by the ICT Co-ordinator.
- Personal computers and devices should not be used for academy related purposes.
- Members of staff must not allow a student to have individual use of a staff account under any circumstances, for any length of time, even if supervised.
- When leaving a computer unattended, it must be ensured that the computer is either logged off, or locked to prevent anyone using another's account (press "Win" & "L").
- Users must not store any sensitive or personal information about staff or students on any portable storage system, such as a USB memory stick, portable hard disk or personal computer. USB memory sticks must be encrypted.
- When publishing or transmitting non-sensitive material outside of the academy, staff must take steps to protect the identity of any student whose parents have requested this.
- If a personal computer is used at home for work purposes, users must ensure that any academy-related sensitive or personal information is secured to prohibit access by any non-member of staff.
- Backups of data kept on any storage system other than the network storage drives should be performed on a regular basis by the user. This includes USB memory sticks (even those owned or issued by the school) or a personal computer.

- School loaned equipment:
    - Ensure that items of portable computer equipment, such as laptops, digital cameras or portable projectors are securely stored in a locked room or cupboard when left unattended.
    - Equipment taken offsite is not insured by the school. If any school computer equipment is taken offsite, it should be ensured that adequate insurance cover has been arranged to cover against loss, damage, or theft. Equipment must not be left in car boots.
    - Ensure personal or work software is not uploaded to school's equipment without the permission of the Headteacher
    - In order to keep accurate asset records, staff laptops must be checked and signed for on an annual basis. Failure to comply will result in re-appropriation of equipment.
    - Laptops must be brought to school every day and when not being used for planning must be used to support student learning and progression.

CONDUCT

- Staff must at all times conduct computer usage professionally, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, gambling related, profit making, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials.
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
- Staff must ensure all Internet activity is appropriate to staff professional activity, including research for professional purposes. Where the system is made available for personal use, the same principles apply
- Staff must respect and not attempt to bypass, security or access restrictions in place on the computer system.
- Staff must not intentionally damage, disable, or otherwise harm the operation of computers.
- Staff must make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive storage of unnecessary files on the network storage areas.
    - Use of printers to produce class sets of materials, instead of using photocopiers.
- Staff should avoid eating or drinking around computer equipment.
- Staff must not use any academy facilities/resources in ways stated within the unacceptable use policy, which can found at the end of this document.

SOCIAL NETWORKING POLICY

INTRODUCTION

The widespread availability and use of social networking applications bring opportunities to understand, engage and communicate with our audiences in new and exciting ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our Academy Community and partners, our legal responsibilities and our reputation.

For example, our use of social networking applications has implications for our duty to safeguard children.

The policy requirements in this document aim to provide this balance to support innovation in ICT, whilst providing a framework of good practice. They apply to all members as defined by Academy representatives.

PURPOSE

The purpose of this policy is to ensure:

- that Flowery Field Primary School, its leaders and governors are not exposed to legal risks.
- that the reputation of Flowery Field Primary School, representatives and Governors at the academy are not adversely affected.
- all children are safeguarded.
- that any users are able to clearly distinguish where information provided via social networking applications is legitimately representative of Flowery Field Primary School.
- The purpose of this guidance is to outline the responsibilities and expected standards of behaviour for all representatives when using social media both inside and outside of work. It forms part of the academy's existing ICT and email security policy.

SCOPE

This policy covers the use of social networking applications by academy representatives, Governors and/or Elected Members and by partners or other third parties on behalf of the Academy.

These groups are referred to collectively as 'Academy representatives' for the purpose of this policy.

The requirements of this policy apply to all uses of social networking applications which are used for any academy or Enquire Learning Trust related purpose and regardless of whether applications are hosted corporately or not. They must also be considered where Academy representatives are contributing in an official capacity to social networking applications provided by external organisations.

Social networking applications include, but are not limited to:
Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Micro blogging' applications. Examples include Twitter, Facebook, MSN, YouTube.
Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All Academy representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the Academy and Enquire Learning Trust Equality and Safeguarding Policies.

Any communication received from children to Academy Representatives must be immediately reported to the Principal – Designated Child Protection Officer and procedures for safeguarding followed.

CONSIDERATIONS

What is Social media?
Social media applies to blogs, microblogs like Facebook, Twitter, Bebo, Linkedln, videos, MySpace, social networks, discussion forums, wikis and other personal webspace. The internet is a fast moving technology and it is impossible to cover all circumstances, however, as a general rule, social media is anything on the internet where content is created and adapted by the people who use the site and which allows two-say conversations.

What role does social media have in the academy?
In academy, communication is encouraged amongst our academy representatives, children and parents. Social media can be a great way to stimulate conversation and discussion as well as sharing information and consulting.

There are legitimate activities when academy representatives can use social media on the internet as part of their work, however, they must do so appropriately in line with these guidelines and the council's academy values.

These guidelines are to protect you and the reputation of the academy. They are not meant to restrict your work or personal use of what is an important method of communication and engagement.

Can academy representatives use social media at work for personal use?
Every academy my take a different approach and it is, therefore, important to understand what is allowed. The Governing Body at this academy does not permit the use of social media on work premises, outside of work time.

What about using social media sites when I'm not in work?
The Governing Body respects an employee's right to a private life. However, they must also ensure that confidentiality and the reputation of the academy are protected.

Even if your social media activities take place outside of work, what you say can have an influence on your ability to conduct your job responsibilities, your work colleagues' abilities to do their jobs, the business and reputation of the academy.

Your personal activities must not undermine the academy's reputation, your professional reputation, or create perceptions of impropriety in the academy, or bring the academy into disrepute in line with Part 2, Section B of the Teachers' Standards 2012.

How to protect yourself and students
The following advice shows best practice for both yourself and the academy.

- Act in accordance with this policy and the Flowery Field Primary School Code of Conduct for Adults.
- Have no secret social contact with students.
- report and record any situation, which you feel, might compromise the school or you own professional standing.
- never give their personal contact details to students or parents, including their any telephone numbers, personal email address, on-line user names and gamer tags other than those utilised professionally.
- Not 'friend' students, parents, ex-parents or ex-students on social networking sites.
- Staff must only use academy emails for academy business. There must be no communication about work on personal emails. This includes file sharing sites; for example Dropbox and YouTube.
- Change your gamer tags and user names if students become aware of it
- Do not use internet or web-based communication channels to send personal messages to a student.

- Do not have images of students stored on personal cameras, devices or home computers.
- Do not make images of students available on the internet, other than through the academy network/website, without permission from parents and senior teachers.
- Do be cautious in your contact with ex-students, as there is still a professional relationship and there may be contact with current students.
- Set your privacy settings. Most social networking sites allow you to control who can see your information. For example, at the bottom of every page on Facebook, there is a link that reads 'privacy'. The linked page is 'a guide to privacy on Facebook', containing the latest privacy functions and policies. Set your privacy settings to "only friends". Settings such as "friends of friends" and "networks and friends" open your content to a wider audience. Your privacy and that of your family, friends, colleagues and students could be compromised.
- Bear in mind that somebody else could post a photo on their profile in which you are named, so think about any photos you appear in. On Facebook, you can 'untag' yourself from a photo. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- Remember humour is relative. For example, posting images and/or text about a recent stag or hen night may be deemed inappropriate. Likewise, a few 'light-hearted' comments and/or images about colleagues or students may not be perceived as such by either the subject(s) of the humour or your employer. The guiding rule is if in doubt, don't post it.
- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.
- Remember that parents and students may access your profile and could, if they find the information and/ or images it contains offensive, complain to your employer.
- You should not 'speak' for the academy (disclose information, publish information, make commitments/comments or engage in activities on behalf of the academy) unless you are specifically authorised to do so by the Headteacher. Any online activities associated with work for the academy should be discussed and approved in advance by your Headteacher.
- Consider that colleagues, including management, might access your profile. Depending on the comments and/or images it contains, you may face disciplinary action.
- Keep your date of birth and home address to yourself.
- Mind your language. Abrupt, inappropriate and unthinking use of language may lead to complaints from colleagues, students, parents and/or management.
- Stop the network provider from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click 'account', then 'privacy settings', then 'search'. Beside 'instant personalisation pilot programme', click 'edit setting'. Make sure the box at the bottom of the screen has not been ticked. To ensure that you do not appear in any adverts, click 'accounts', then 'account settings', then 'Facebook adverts'. Select 'No one' on the 'allow ads on platform pages to show my information to' and 'show my social actions in Facebook ads to'.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

USE OF EMAIL

All members of staff with a computer account are provided with an email address for communication, both internally and with other email users outside the academy.

E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. Staff must be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for e-mail. Staff should regularly check email and delete older mail when it is no longer required.

SUPERVISION OF STUDENT USE

- Students must be supervised at all times when using academy computer equipment. When arranging use of computer facilities for students, staff must ensure supervision is available.
- Supervising staff are responsible for ensuring that the Student ICT Policy is enforced.
- Supervising staff must ensure they have read and understand the separate guidelines on e-safety, which pertains to the child protection issues of computer use by students.

E-Safety Policy

Principles and purpose

New technologies have become integral to the lives of children and young people in today's society, both within and outside their school lives. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Students have an entitlement to safe internet access at all times.

The use of these technologies can put students at risk, some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, sharing of personal information
- Risk of being subject to grooming by those with whom they make contact
- The sharing and distribution of personal images without their consent
- Inappropriate communication and contact with others
- Cyber-bullying Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of e-information
- Plagiarism and copyright infringement
- Illegal downloading of music and video files
- Excessive use impacting on social and emotional development
- Vulnerability to radicalisation.

Scope of the Policy

This policy applies to all employees and students wherever they may be, both at school or elsewhere such as at home when accessing systems which the school is responsible for.

E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages across the curriculum;

- The e-safety curriculum is provided as part of our on-going integrated curriculum including Computing and PHSE.
- The Whizz Kids provide student leadership of E-safety in partnership with the E-safety committee.
- Key e-safety messages are reinforced as part of our assembly pastoral activities.
- Students are taught in all lessons to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information.
- Students are helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies the internet and mobile devices.

Guidance for parents

Many parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities and celebrations
- Website, social media, notices.
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites e.g. www.saferinternet.org.uk/ and www.childnet.com/parents-and-carers

CYBER BULLYING

Definition

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend themselves.

Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.

Cyber-bullying, is bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones and devices
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, including but not limited to Facebook, Youtube, Snapchat and Ratemyteacher

At Flowery Field Primary School we have zero tolerance of any form of bullying.

LEGAL ISSUES IN RELATION TO CYBERBULLYING

Cyber-bullying is generally criminal in character.
It is unlawful to disseminate defamatory information in any media including internet sites.
Section 127 of the Communications Act 2003 makes it an offence to send, by public means of a public electronic communications network, a message or other matter that is grossly offensive or one of an indecent, obscene or menacing character.
The Protection from Harassment Act 1997 makes it an offence to knowingly pursue any course of conduct amounting to harassment.

The wider search powers included in the Education Act 2011 give teachers stronger powers to tackle cyber-bullying by providing a specific power to search for and, if necessary, delete inappropriate images (or files) on electronic devices, including mobile phones.

Students are kept up to date in both the proper use of technology and about the serious consequences of cyber-bullying through the integrated curriculum which includes PSHE and computing learning sessions alongside assemblies, the Whizz Kids, website and involvement in events such as Anti-bullying Week and Safer Internet day.
All staff are aware of the need to respond effectively to reports of cyber-bullying or in line with the academy's anti-bullying policy

At Flowery Field Primary School we support victims of cyberbullying, and when necessary, will work with the Police to detect those involved in criminal acts.
If cyberbullying is evident this must be reported as per the Anti-bullying Policy immediately to the Principal

GUIDANCE FOR STAFF

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile phones and devices:

- Ask the student to show you the mobile phone
- Note clearly everything on the screen relating to an inappropriate text message or image, to include the date, time and names
- Make a transcript of a spoken message, again record date, times and names
- Tell the student to save the message/image. Take a screen shot.
- If the nature of the data is explicit do not forward the material as this could be illegal sharing of explicit images.
- Reassure the student.
- If a safeguarding concern is raised that this must be raised immediately with the Child Protection Office as outlined in the Safeguarding and Child Protection Policy.
- Immediately inform the Principal or member of Senior Leadership Team who will instigate the anti-bullying policy.

Computers:

- Ask the student to get up on-screen the material in question.
- Ask the student to save the material or take a screen shot.
- Do not print off or electronically share any explicit content or images.
- Re-assure the student
- Immediately inform the Principal or member of Senior Leadership Team who will instigate the anti-bullying policy.

GUIDANCE FOR STUDENTS

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible.
- Do not answer abusive messages or emails but log and report them
- Do not delete anything (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying)
- Do not give out personal IT details
- Never reply to someone you do not know

- Stay in public areas in chat rooms

GUIDANCE FOR PARENTS

- It is vital that parents and the academy work together to ensure that all students are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. We inform parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying via the website and news alerts.
- Parents can help by making sure their child understands the school's policy and, above all, how seriously St Richard's takes incidents of cyber-bullying
- Parents should also explain to their sons or daughters legal issues relating to cyberbullying
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (by saving an offensive text on their or their child's mobile phone, mobile device or computer) Avoid deleting information. Parents should contact the Principal as soon as possible.
- If the incident outside of the normal school day and calendar the academy reserves the right to take action against bullying perpetrated outside the school which spills over into the school.
- Further up to date advice on cyberbullying and e-safety can be found on the academy website.

ACADEMY STAFF AND CYBER BULLYING

All school staff are in a position of trust, and there are expectations that they will act in a professional manner at all times.

- Ensure you understand your school's policies on the use of social media, Childnet.com 'Using Technology' guide has more information on what to be aware of.
- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by students.
- Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date. Advice can be found on the Safer-internet advice and resources for parents and carers.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online it is much easier to deal with this as soon as it appears. The UK Safer Internet Centre's Reputation mini-site has more information on this.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Use your school email address for school business and personal email address for your private life; do not mix the two. If you are bullied online
- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current student or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to

make sure they know how to raise this appropriately. They can request that the person removes the offending comments.

- If they refuse, it should be an organisational decision what to do next – either the school or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies for example, The UK Safer Internet Centre.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the school may consider contacting the local police. Online harassment is a crime.
- The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

PRIVACY

- Use of the academy computer system, including email accounts and storage areas provided for staff use, may be subject to monitoring by the academy to ensure compliance with this ICT Policy and applicable laws. In particular, the academy does keep a complete record of all websites visited on the Internet by both students and staff; however, usernames and passwords used are NOT monitored or recorded.
- Staff will not store personal information sensitive or otherwise on the academy computer system that is unrelated to academy activities (such as personal passwords, photographs, or financial information).
- The academy may also use measures to audit use of computer systems for performance and diagnostic purposes.

CONFIDENTIALITY AND COPYRIGHT

- Work and ownership rights of people outside the academy, as well as other staff or students, should be respected.
- Staff members are also responsible for complying with copyright laws and licenses that may apply to software, files, graphics, documents, messages and any other material which may be used, downloaded or copied.
- An ICT Technician must be consulted before the placing of any order relating to computer hardware or software or before obtaining and using any software believed to be free. This is to check that the intended use by the academy is permitted under copyright law, as well as to check compatibility and discuss any other implications that the purchase may have. The claims of suppliers should not be trusted, as they do not have specific knowledge of the academy computer system.
- Students are be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

REPORTING PROBLEMS WITH THE COMPUTER SYSTEM

It is the job of the ICT technician to ensure that the academy computer system is working optimally at all times and that any faults are rectified as soon as possible. In order to sustain this:

- Staff should report any problems that need attention to an ICT Technician as soon as possible by using the online “ticket raising” facility or by informing our office staff.

- If a computer has been affected by a virus or other malware or even suspected to have been, staff should report this to an ICT Technician immediately.
- Lost documents or files should be reported as soon as possible. The longer a data loss problem goes unreported, the lesser the chances of data recovery.

REPORTING BREACHES OF THIS POLICY

All members of staff have a duty to ensure this Staff ICT Policy is followed. Any breach of this policy should be immediately reported to the ICT co-ordinator or a member of SLT (refer to whistle blowing policy).
In particular, the following should be reported:

- Any website which is accessible from within academy that is felt to be inappropriate for staff or students.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, network areas, USB drives etc. and may include pictures, videos, applications etc.
- Any breaches, or attempted breaches, of computer security (i.e. password sharing).
- Any instance of bullying or harassment suffered from/by any member of staff, or student via the academy computer system.

Reports should be made either via email or directly to an appropriate member of staff. All reports will be treated confidentially.

UNACCEPTABLE USE POLICY

Any use that is illegal, against Academy policy or contrary to the Academy's best interest, particularly:

- If it is a non-Academy business use and for an **unacceptable purpose**
- If it is a **frequent and/or time consuming non-business use of email, internet or telephones**
- If it contains **unacceptable** types of **content**

UNACCEPTABLE PURPOSES

Examples of non-Academy business use of the internet, email & telephone facilities which are unacceptable at any time, include but are not limited to:

- Any use associated with running a business activity, whether for profit or not.
- Computer crimes, such as hacking.
- Harassment of any kind.
- Downloading music and films.
- Any use of internet facilities which would allow unacceptable non-business use of Academy systems to be concealed.
- Accessing sites which are blocked for reasons of legality or taste without approval.
- Using your work email address for personal purposes, such as:
    - Subscribing to email newsletters which are not work related.
    - Using as a contact address on websites e.g. selling goods and services.
    - Use of social media web sites such as Twitter and Facebook.

FREQUENT AND/OR TIME CONSUMING NON BUSINESS USE OF EMAILS, INTERNET AND TELEPHONES

Non-business use of these facilities should not take place in work time. Some examples of frequent use of the internet, email & telephone facilities which may be non-essential business uses, perhaps occurring as a result of unsolicited emails, include, but are not limited to:

- Excessive visits to sports results, commentaries and news sites.
- Personal non-Academy business distribution lists greater than 5 addresses.
- Bulk personal internal or external emails.
- Participating in chain letters and petitions.
- Sending non-Academy business emails with large attachments.
- Chatting or distributing jokes via email or text.

LAPTOP AND MOBILE DEVICE USAGE POLICY

Purpose

The policy outlines the responsibilities that Flowery Field Primary School staff must accept when they are issued a laptop and/or mobile device.

Laptop Care and Precautions

- All members of staff must take appropriate steps to protect their laptop from theft:
    - Laptops should not be left in an unattended office without closing and locking the door.
    - Laptops should not be left out overnight in offices, and should always be locked away.
    - Laptops, where possible, should not be left unattended in a parked car. On those occasions where there is no alternative, the laptop should be locked in the boot.
- Laptops should not be used in environments that might increase the likelihood of damage.
- Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage.
- All members of staff are accountable for all network and systems access under their user ID, passwords should be kept absolutely secret. It should never be shared with anyone.
- School laptops are provided for official use by members of staff. Laptops must not be loaned or be allowed to be used by others.
- Any damage or loss must be reported to school.
- School laptops and mobile devices should be brought to school every day (teachers and teaching assistants) so children can access ICT in small group work/1:1 work or larger group work.

Data Encryption

It is a legal requirement of the Data Protection Act 1998 to protect and secure personal data. The Information Commissioner's Office (ICO) recommends that portable and mobile devices (including media) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

- Sensitive information refers to any data that is protected by school policy, or by any local, or national laws or regulations. This includes but is not limited to;
    - Education records.
    - Personally identifiable information.
    - Confidential internal school information.

If sensitive data needs to be used and stored on a laptop the hard drive of the laptop must be encrypted. Please contact IT technician if you require encryption to be installed.

Anyone needing to carry sensitive data should contact the IT technician for information regarding the purchase and use of an encrypted USB device.

Virus Protection

- Viruses are a major threat to the school network and laptops are particularly vulnerable if their antivirus software is not kept up to date.
- The antivirus software must be updated at least monthly. The easiest way of doing this is simply to log onto the school network allowing the automatic update process to run.
- Email attachments are one of the main sources of computer viruses. Avoid opening any email attachments unless they are expected from a legitimate source.
- Report any security incidents (such as virus infections) promptly to the IT technician in order to minimise the risk of damage.
- Under no circumstances must the antivirus software installed on the laptop be removed or replaced with an alternative version by members of staff.

Software Installations

- Under no circumstances must any of the preinstalled software be removed from the school laptops.
- Members of staff are not permitted to download, install or use unauthorized or unlicensed software programs.
- Any software that is required to be installed must be installed through the IT technician.

Legislation

All laptop and mobile device users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- Data Protection Acts 1994 and 1998
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

7.2 Where it is believed that a member of staff is in breach of legislation appropriate action will be taken.

8. Sanctions

In the event that this ICT Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.

Related policies and guidance

- Safeguarding and Child Protection Policy
- Antibullying Policy
- Student ICT Acceptable Usage Form
- Behaviour Policy
- Enquire Learning Trust Disciplinary Procedures