Policy for the Acceptable Use of IT, the Internet and Personal Data

1. Requirements

1.1 Change Record

Issue	Date	Author	Description
0.1	December 2014	P Atkin	Initial Draft
0.2	January 2015	P Atkin	Second draft following LT review
1.0	March 2015	P Atkin	Ratification by Governing Body
1.1	November 2017	P Atkin	Update
2.0	December 2017	P Atkin	Ratified by Governing Body

Note: All issues except those of the form 'X.0' are draft.

1.2 Equality Statement

In developing and reviewing this policy we have carefully considered its impact on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

1.3 Approval and Review

This policy was approved by the Governing Body on 6/12/17. It is due for review in the Autumn Term 2019.

2. Aims and Values

Our aim is to develop learners who are confident, considerate and safe users of IT. We aim to meet the requirements of the National Curriculum and Early Years Foundation Stage, offering opportunities for pupils to evaluate the use and impact of IT and computing in their learning.

This policy outlines what Fowlmere Primary School believes are the most appropriate ways for pupils and staff to make use of technology including the internet, mobile devices, social media and messaging.

It explains how Fowlmere Primary School strives to meet its legal and moral responsibilities.

3. Working Online

Internet access raises educational standards by creating valuable opportunities to extend the range of information, resources and people which children can encounter, e.g. museums, art galleries, world-wide educational resources, cultural and information exchanges between students locally and world-wide.

It provides opportunities for pupils to access resources and collaborate outside of the traditional boundaries of school, for example working at home outside of school time.

It supports the professional work of staff and enhances the school's management information and business administration systems, for example through access to educational materials and good curriculum practice.

3.1 Internet Access

Internet access will provide effective learning for children by:

- teachers setting clear objectives and expectations for internet use;
- teachers selecting and supervising access to sites which will support the learning outcomes planned for pupils' age and maturity;
- filtering appropriate to primary age pupils through the LA provider;
- pupils being educated in taking responsibility for their own internet access;
- specific teaching of search techniques;
- staff bookmarking approved sites.

3.2 Assessing Internet Content

At an appropriate age, children will be:

- taught ways to validate information before accepting that it is necessarily accurate;
- encouraged to tell a member of staff immediately if they encounter any material which is inappropriate or makes them feel uncomfortable.

Staff should check any website they recommend to pupils carefully to ensure appropriate content. Careful consideration should be given where sites accept user comment which can change regularly and is rarely subject to moderation.

3.3 YouTube and other Video Sharing Sites

Sites such as YouTube offer opportunities to present ideas and information though video easily and conveniently. YouTube is unavailable to pupils through the county proxy servers (pupils are redirected to the Education channel) but is available to teaching staff.

Staff should be aware of the following when using YouTube:

- content is unmoderated and unfiltered, therefore should be checked by staff **in its entirety** to ensure that it is suitable for viewing in the classroom
- sidebars, adverts, suggestions and user comments may all contain unsuitable material and should be checked carefully before the decision to use a video is taken
- copyright should be respected

3.4 Electronic Mail (e-mail), Internet Chat & Social Media

E-mail provides an opportunity to communicate quickly and effectively with a wide range of people and places which have otherwise been beyond the reach of pupils, eg authors, pupils in other localities, etc. As a general rule, the use of email for the curriculum will be managed at a class level, ie one account used for the whole class, however children using the school's learning platform, eSchools, will have access to individual internal email.

Public real-time chat will not be used by individual pupils. External social media sites, such as Facebook and Twitter will also not be used.

In addition:

- incoming mail will be regarded as public;
- children will not have individual external email addresses
- local internet forums will be closely supervised by the class teacher
- pupils will be taught how to safely manage their internal email

3.5 Web Publishing

The school regularly publishes content on the web, for example, through its own website. When publishing such material:

- the Headteacher will delegate editorial responsibility to a staff member to ensure that content is accurate and quality of presentation is maintained;
- the point of contact on the web site should be the school address and telephone number, home information or individual e-mail identities will not be published;
- first names of pupils only will be used on the website – parents may request that a pseudonym be used where a pupil is at risk of identification through their first name, or that their name not be used at all;
- the Headteacher holds a list of children whose photograph should not appear online where parental consent for this has been withdrawn. All staff must be aware of this list when submitting photographs for online publication.

See Appendix 2 – Guidelines for Publishing in the Community

3.6 Virtual Learning Environments (VLEs) - eSchools

Virtual Learning Environments provide a secure online environment in which children can work and collaborate. Our school uses the VLE from eSchools which provides access to internal email, messaging and personal blogging. Pupils can access information posted by staff and by other children. This service is open only to staff, pupils and families of Fowlmere Primary School.

The eSchools VLE allows individual class teachers to manage online communities at class and group levels. Within these communities children can be given access to the following:

- A secure internal email account, allowing them to send and receive emails **only** to and from other users within the Fowlmere eSchools community.
- Personal and class online filespace in which work and files can be saved and accessed in and out of school (allowing increased opportunities for extended working.)
- A range of other communication tools such as blogs, forums and instant messaging.
- Access to project information and websites.

The following guidance should be followed when using eSchools:

- Children must be familiar with the Code of Conduct for using a VLE given in Appendix 4. Staff should start any new eSchools project with a reminder of this code of conduct.
- Staff must take particular care to maintain a protective ethos (as defined in the school's Child Protection Policy) when communicating with children within eSchools and to ensure that they do not attempt to make contact with children outside of eSchools. The headteacher and Computing subject leader will monitor the comments and communications made within eSchools in order to ensure this is the case.
- Staff should be aware of the potential for online or cyber-bullying and act according to the school's Anti-Bullying Policy.
- Staff are responsible for monitoring the use of forums or other collaborative tools within the projects they manage to ensure appropriate use.

3.7 Internet Telephony / VOIP / Video Calls

Software such as Skype allows children to communicate directly with schools and individuals in other localities freely and with the possibility of seeing the people with whom they are talking through video calls. Such activities must always be part of the school's curriculum and supervised by a teacher. Webcams should be disconnected from computers after use and integrated webcams, covered.

3.8 Use of Tablet Computers (iPads)

The school has a small set of iPads available to pupils and also has two staff iPads. These are set up to use the same internet filtering as other equipment in the school. In particular, the pupil iPads have the following security settings enabled:

- Restrictions are in place, using a passcode, in order to:
  - deny access to Facetime and iTunes store
  - prohibit the installation and deletion of apps as well as In-app purchases
  - restrict film content to "U" certification
  - deny access to TV content (as there is no certification system in place)
  - restrict access to music content

3.9 Staff Internet Use

Internet and e-mail provide valuable opportunities for teachers and support staff to access resources and information necessary for the planning and delivery of high-quality lessons and activities. This is facilitated by:

- Access to the internet at school
- Provision of e-mail for all staff

All staff must ensure that their internet access is inline with the guidance set out in Appendix 3 – Acceptable ICT Use for Staff.

3.10 Governors' Email

Governors use email to communicate between meetings, eg to agree meeting agendas, and circulate papers for forthcoming meetings. Whilst much governor activity eventually enters the public domain, some items remain confidential, and papers and minutes should be confidential until approved by the whole governing body, or appropriate committee. As such, governors are reminded that:

- Governors' business should always be conducted in properly constituted meetings and never by email
- Governors are expected to use their school-provided email address for governors' communication. This is to avoid accidental sharing of confidential information, eg though accidental forwarding, or shared family emails.
- Governors subject to a formal complaint may be expected to provide an "audit trail" of email communication

3.11 New Internet Applications

New applications are being developed all the time; however, most begin without the needs of young users and their security being considered, therefore new applications will be thoroughly tested before pupils are given access.

4. Internet Safety

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use. At Fowlmere Primary School, access to the internet is supervised at all times. Parents will be informed that children will be provided with supervised Internet access and will be asked to discuss appropriate use with their children.

4.1 Range of Access

Pupil internet access will reflect the age and maturity of children.

It is anticipated that:

- in Foundation Stage and at KS1, pupils access to the internet will be through bookmarked pages. For example children may have access to interactive texts, phonics games or maths games.
- at Key Stage 2, pupils will continue to work from bookmarked sites, but will also be expected to use increasingly accurate searches online, discriminating between the validity of their results.

4.2 Unsuitable Internet Material

In common with other media such as magazines, books and videos, some material available via the Internet is unsuitable for pupils. The school will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. The LA Internet Provider will see that checks are made to ensure that the filtering methods selected are effective.

However, due to the scale and linked nature of information available via the Internet, it is not possible to totally guarantee that unsuitable material will never appear on screen. Neither the school nor Cambridgeshire County Council can accept liability for the material accessed, or any consequences thereof.

The use of computers without permission and for purposes not agreed by the school, could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks include:

- content filtering at the service provider level
- content blocking at the school level through the use of dedicated network hardware
- teachers evaluating and bookmarking appropriate sites before teaching
- teachers giving pupils clear guidance about internet access
- displaying internet rules beside all computers
- an annual review of responsible Internet use both at school and home as part of the ICT curriculum and class rules
- supervised access at all times – pupils must not be given internet access without adult supervision
- logging and monitoring previous site access
- unsuitable material which passes the content filtering being reported to the service provider

These strategies will be reviewed on a regular basis.

Staff, parents and governors will work to establish agreement that every reasonable measure is being taken.

The school will work in partnership with the LA, DfE, Internet Service Provider and parents, to ensure systems which protect pupils are reviewed and improved.

5. ICT Equipment

5.1 Available ICT Equipment

The school makes as much equipment as possible, within its resources, available to staff and pupils. This includes laptops, desktops, tablets and cameras, as well as a range of other curriculum resources.

This means that there is no requirement for staff to make use of their own IT equipment. In particular, staff must not use their own laptops, phones, tablet computers or cameras in lessons without the explicit permission of the headteacher and Computing Subject Leader.

6. Handling Personal Data

As the use of ICT has increased in schools, so has the amount of personal data held on pupils and staff. Examples of the data held by the school on its IT systems includes:

- contact details, ethnicity and basic medical information
- records of attendance and absence
- reports for parents, transfer schools, health and other professionals
- assessment data, test scores and results at both pupil and question level
- records of pupil activity, such as library books borrowed or school meals taken

There must be a clear, identifiable purpose to the data held on pupils at the school. The school acts within current data protection legislation and is committed to keeping such data securely.

The school has worked with Cambridgeshire LA to issue a fair processing notice (FPN) to all parents at Layer 1. Layer 2 and Layer 3 information for parents is available on request. The school shares information on a pupil level with the DfE, STA and LA and this is explained in the school's FPN.

The school operates a number of procedures to protect personal data. These include:

- Centrally managed server storage of data, supported by Cambridgeshire ICT service to agreed standards
- Central Hosting of Pupil SIMS Data
- A staff ICT use agreement which details individual staff members responsibilities with regard to personal data
- Risk Assessments for off-site storage of data
- File encryption when transferring data outside secure networks, eg to/from the NHS

6.1 User Profiles

All IT users at Fowlmere Primary School have their own user profile, which is password protected. Users should keep the password secret at all times. If a password becomes known they should inform the Computing subject leader.

At no time, should any user use, or encourage others to use, user profiles which are not assigned to them. In particular, staff must not allow their user profile to be used by pupils, under any circumstances.

Staff must log off their user profile, or lock their computer when away from it for long periods of time.

Supply teachers are given a guest login which only allows them to access shared files.

6.2 Sharing sensitive data

When sharing files containing pupil-level or staff-level data outside of Cambridgeshire's internal email system or network, files must be password encrypted. These files should not be saved onto storage devices. Therefore:

- Encryption is not required when:
  - sharing information within the school (including shared folders which have staff-only access)
  - emailing files to @cambridgeshire.gov.uk and @schoolname.cambs.sch.uk email addresses
  - Sending data though S2S or COLLECT secure data transfer system
  - There is no pupil-or staff-level data in the file, eg it is planning, worksheets, etc
- Encryption is required when:

- transferring pupil- or staff-level data outside the county network, eg to @nhs.net email addresses, @epm.co.uk
- Using cloud-based storage (after appropriate risk assessment)

6.3 Deleting Files

While children and staff remain part of the Folwmere School Community, files, videos and digital images will be stored centrally on the server. These files will be stored on the school computers for up to one academic year upon leaving the school community. It is the responsibility of the Computing subject leader to delete appropriate files.

In some exceptional circumstances, examples of work or photographs of past members of the community may be required for archive purposes. It is agreed that files kept as a subject profile should be deleted after five years. Some photos may be required for the maintenance of the school collective memory.

6.4 Use of School Laptops

Laptops are provided for teachers' use in fulfilling their professional role. They remain school property and are distributed at the discretion of the Headteacher.

Their use is subject to the following guidelines:

- Teachers should not install third-party software onto the laptops. If software needs to be installed they should inform the Computing subject leader.
- Teachers may use school laptops for e-mail and internet access. However they should follow the guidance set out in 'Acceptable IT Use For Staff'.
- Teachers must ensure the safety of the IT equipment provided to them. When using laptops outside of the school building, teachers must ensure that these are kept out of public view and are appropriately secure; laptops must not be left unattended in vehicles.
- Where a member of staff is likely to be away from school for an extended period through illness, professional development (such as secondment etc.) arrangements must be made for any portable equipment in their care to be returned for school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.
- Any costs generated by the user at home, such as broadband bills etc. are the responsibility of the user.

6.5 Use of Cloud-Based Storage Systems

The school makes use of cloud-based storage to facilitate efficient working. In particular:

- Central Hosting stores files for staff and the school in general
- The school's eSchool website hosts certain governor documents for secure access
- Dropbox and Google Drive is used to share planning, resources, the staff handbook and policies between staff

Pupil-level data of any kind must only be stored in a system covered by the EU Data Protection Act. The US Safe Harbor designation is self-certificated and is **not** equivalent to DPA compliance.

Simple steps can be taken to reduce risk, eg use of pupil initials by teachers in planning.

The level of encryption and use of these services, should reflect the nature of the data involved:

Data	Rationale	Approval
Low- to moderate-level pupil data, eg class groupings, class lists, text-based reports	The data is sensitive but does not identify pupils outside the school community	Use is approved; Encryption required
High-level pupil data, eg medical reports, CAFs, Statements, photographs	The data is highly sensitive and usually identifies pupils by full name and address	**Use is not approved**

Staff must not use personal accounts to access these services.

6.6 Use of Other Online Data Systems

The school makes use of a number of third-party online systems to manage pupil and staff-level data. These are all sourced from reputable and EU DPA compliant providers whose data and privacy policies have been evaluated. Examples of such providers include:

- **EPM Portal** – management of staff contracts, payroll, absence data etc
- **Atlantic Data DBS Portal** – management of DBS disclosures for staff and volunteers
- **Provision Map** – management of pupil learning plans, behaviour logs and SEND provisions
- **Schools Library Service (easylib)** – management of school library and borrowers catalogue

7. Copyright

Pupils, staff and parents are expected to observe copyright regulations in respect of photocopy and electronic copying; this includes music and video delivered electronically. We insist that all software used in school is suitably licensed and this is monitored annually.

8. Complaints

The responsibility for handling any complaints under this policy will be given to members of the Leadership Team. The school's general complaints procedure will apply.

Appendix 1 – Code of Practice for Pupil IT Use

The following information is shared with pupils on the desktop of all pupil logins.

Appendix 2 - Guidelines for Publishing in the Community

These guidelines are for the protection of pupils when the school wishes to publish in the wider community.

In all cases, the addresses, telephone numbers, or e-mail addresses of individual members of our community are not circulated by the school.

Such publications can be grouped into 3 categories.

Publishing to the School Community

Publications which are circulated to parents, pupils, governors and staff with a direct connection with the school include:

- letters to parents
- Newsletters (for school circulation)
- leaflets (homework leaflet, etc.)

Pupils may be identified by both their first name and their surname, as this information is already common knowledge within the school community. They may also be identified by their year group.

Where the naming of a pupil in any way may lead to a disclosure of other information about a pupil's personal circumstances, for example, medical information or Additional Educational Needs, they should not be named at all. Specific information about such a pupil should not be given in this context.

Photographs of pupils may be published, but should not identify a child by their first name.

Publishing to the Local Community

Including:

- Parish Magazine
- Local Newspapers

Photographs of pupils may be published. In general they should not identify a child by their first name, unless explicit parental permission for this has been obtained. It is the school's responsibility to ensure that external publishers are aware of the school's publication guidelines and to establish whether such publications will be available on the internet.

Usually, the school would allow the publication of a pupil's second name in a local newspaper, within the text, unless a parent had specifically asked for this not to happen, or the school is aware of any reason why this should not happen.

If such publications are to be published on the internet, the following section applies.

Publishing on the Internet

Including:

- School Website
- Newsletters (web edition)

The school publishes photographs of children online, for example, on the school website homepage. Group photographs or "action shots" at a distance are preferred to easily identified individuals. Children should not be named in photographs.

Within text children may be named by their first name and year group/class only. In exceptional circumstances, parents may request that their child be given a pseudonym, or that they not be named at all. Parents are informed of this policy on their child's admission and it is their responsibility to inform the school of such a request.

Appendix 3 – Acceptable IT Use Statement for Staff

Acceptable IT Use

For Staff

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The Policy for the Acceptable use of IT, the Internet and Personal Data has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable IT Use Statement and return it to the Computing Subject Leader.

General Use of IT:

Use of the school's IT equipment, (including laptops, tablets, cameras or internet connection) must be in line with the expectations of professional conduct irrespective of whether the use takes place within or outside of the school. In particular:

- communications (whether by email, chat or posting online messages) using the school or local authority's systems or equipment must meet the same standards as for other forms of written communication within the school
- use of the school or the local authority's systems or equipment to access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden
- use for personal financial gain, gambling, political purposes or advertising is forbidden
- you must only use your own, allocated user profile and login details, and must not let other users (including family members and friends) access systems using them. If you suspect that someone else knows your password you must change it immediately
- any activity that threatens the integrity of the school IT systems, or activity that attacks or corrupts other systems, is forbidden
- users are responsible for all e-mails or messages sent and for contacts made that may result in e-mails being received
- copyright of materials must be respected
- posting anonymous messages and forwarding chain letters is forbidden
- you must treat as confidential, any information which you have access to using the schools IT systems; you must not copy, disseminate or modify such information without explicit permission from the headteacher
- you must not install or run software which is not authorised by the school; nor copy school software for your own personal use

Security of Personal Data:

- Any file which includes data on an identifiable individual members of our school community (for example, test data, school reports, contact details, performance management) must be saved within an individual staff member's 'Documents' library. If this file is to be shared with other staff members it should be password protected with a secure password. Such files should never be saved on external storage devices, such as USB keys.
- School laptops contain a large amount of personal data. You must take reasonable precautions for the security of the portable hardware in your care. In particular:
  - laptops must not be left in public view or left in a vehicle, even for a short period of time

eSchools Learning Platforms:

Learning Platforms provide excellent opportunities for collaborative learning, however staff must take particular care when communicating with pupils and families in this way. Specifically you must:

- consider the different interpretation which may be put on your online comments when read by different users
- never contact, or communicate electronically with a pupil outside of the VLE
- monitor the classes and projects that you manage for appropriate use in line with the school's guidance and inform the ICT subject leader of any breaches of this guidance. Print copies of any material breaching guidance before deleting it immediately
- ensure that information is accurate and to a high standard, modelling what we expect from children

Full Name: _____

Signed:_____ Dated:_____

Appendix 4 - Code of Conduct for Using a VLE

- I will only use my own login and password, and I will not let anyone else use it. This includes members of my family and friends.
- If I think someone else knows my login and password I will tell my teacher
- I will only leave polite messages or feedback or send polite emails
- I will tell my teacher if I read a comment which makes me feel unhappy or uncomfortable
- I will not share my telephone number, address or email with anyone, in the same way as I wouldn't online.
- I will not use photographs of myself in a public profile.