Policy for the Acceptable Use of IT, the Internet and Communication Technologies

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
2.1	November 2020	P Atkin	Update
3.0	December 2020	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 2 December 2020. It is due for review in the Autumn Term 2022.

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 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

Maximising YouTube videos prior to screen sharing or embedding content in a VLE can minimise, though not eliminate. Some of these risks.

3.4 Email, 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 messaging.

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 by pupils.

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 learning platform messaging

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 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 messaging account, allowing them to send and receive messages **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. The school accepts that monitoring of pupil messages can only be periodic. Pupil must be taught to report message content which is inappropriate.

3.7 Virtual Learning Environments (VLEs) – Microsoft Education 365

Our school uses the Microsoft Education 365 platform which provides access to Microsoft's suite of online tools, collaborative tools, internal messaging, shared and individual filespace, and opportunities to communicate directly with the class teacher. . Pupils can access information shared by staff and shared by other children. This service is open only to staff and pupils of Fowlmere Primary School although there are equivalent spaces for governors and staff alone.

Education 365 allows individual class teachers to manage online teams at class and group levels. Within these communities children can be given access to the following:

- A secure internal message board, allowing them to send and receive messages **only** to and from other users within the team.
- 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.)
- The full suite of Microsoft applications – Word, Excel, PowerPoint, OneNote, Teams, etc
- Access to project information, activities, assessments and websites.

The following guidance should be followed when using Education 365:

- Children must be familiar with the Code of Conduct for using a VLE given in Appendix 4. Staff should start any new 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 Safeguarding and Child Protection Policy) when communicating with children within Education 365 and to ensure that they do not attempt to make contact with children outside of the platform. The headteacher and Computing subject leader will monitor the comments and communications made 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 message boards or other collaborative tools within the projects they manage to ensure appropriate use. The school accepts that monitoring of pupil messages can only be periodic. Pupil must be taught to report message content which is inappropriate.

3.8 Internet Telephony / Video Calls

Software such as Microsoft Teams 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. No child should be making a video call to an individual unsupervised.

3.9 Staff Internet Use

Internet, e-mail and Microsoft Teams 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
- Provision of Microsoft 365 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 and Microsoft Teams 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/Microsoft login 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 electronic 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 takes place as part of curriculum lessons, or extra-curricular activities (such as Code Club). As such, it takes place within a purposeful and structured environment. Parents will be informed that children will be provided with such 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 support 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
- teachers evaluating and bookmarking appropriate sites before teaching
- teachers giving pupils clear guidance about internet access
- displaying internet rules in the classroom
- an annual review of responsible Internet use both at school and home as part of the Computing curriculum and class rules
- pupil access is restricted to times when there is an adult present in the room
- 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.

5.2 Loans

In certain circumstances the school may loan IT equipment to a family – for example, to enable a child with limited resources to access opportunities which may be available to the majority. This is entirely at the headteacher's discretion and would be tied to a particular project, not an open-ended loan.

Teachers should discuss equipment loans with the headteacher if they identify a need.

Equipment loaned to families still belongs to the school and a loan agreement, including acceptable use, should be drawn up between the parties. The school's IT support will prepare the equipment for use, which includes ensuring that there is no access to sensitive data or any breach of licencing conditions.

6. Security

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 and take steps to have the password reset (either themselves or through the schools IT Support Provider)

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.

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 File Storage

All school files are stored in the school's secure SharePoint site. For most users this is a transparent process as school devices are set up in this way. Some documents are stored with approved third-party providers, for example Bromcom or MyConcern.

Files containing personal data or sensitive personal data, must not be stored elsewhere, for example on external drives, USB keys or other cloud-based storage systems. The risk of data loss can be reduced by reviewing the need for including personal data in a file – for example, pupil initials can be used in school planning.

The use of collaborative or shared file space should be used in preference to emailing files. Staff should take care to ensure that files are saved in spaces with appropriate permissions – for example confidential staff documents (such as appraisals) are not saved in Staff Share.

Information about how long files are stored for can be found in the school's Data Retention Policy.

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.

7. Copyright

Pupils, staff and parents are expected to observe copyright regulations in respect of photocopying 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 a regular basis.

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.

Parents must give consent for the use of their child's image in any of the categories below. This consent is granular – ie applies to each category individually. Parents can mange their consents in Bromcom MyChildatSchool. The guidelines below assume consent has been given.

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.

The "publisher" is responsible for ensuring the correct consents are in place.

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.

The "publisher" is responsible for ensuring the correct consents are in place.

Publishing on the Internet (static, non-social, media)

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 (which should not be able to be used to identify children in any photograph) 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.

The “publisher” is responsible for ensuring the correct consents are in place.

Publishing to Social Media

Separate parental consent exists for publishing to dynamic content, such as social media.

The school publishes photographs of children on social media, for example, on Facebook and Twitter. Group photographs or “action shots” at a distance should be used wherever possible. Children in photographs should not be named.

Within text (which should not be able to be used to identify children in any photograph) 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.

The “publisher” is responsible for ensuring the correct consents are in place.

Appendix 3 – Acceptable IT Use Statement 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 Communication Technologies has been drawn up to protect all parties – the pupils, 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 off a copy of this Acceptable IT Use Statement as part of the annual sign-off of documents on MyConcern.

General Use of IT:

Use of the school's IT equipment, (including, but not limited to, 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 school's 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 or school SharePoint site. If this file is to be shared with external agencies 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
- Staff must ensure that they have an up-to-date list of consents for sharing photographs and videos of children.

Microsoft Education 365 and 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 Computing subject leader of any breaches of this guidance. Print (or PDF) 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

- Always ask a grown up before you use the internet.
- Use your own login and password. Never use someone else's login details and don't give yours to someone else.
- Never share phone numbers, addresses or other contact details. In our VLE you can share photos or pictures of things you have made, learnt or done.
- When writing or posting messages, remember to THINK before you post –

  T – Is it True?
  H – Is it Helpful?
  I – Inspiring?
  N – Is it Necessary?
  K – Is it Kind?

  Remember that everything you post can be seen by other people in the school – make sure it is appropriate.

- Always tell a grown up if you feel scared or unhappy about anything. You can use the whistle to let a teacher know about something that is worrying you.