
# Policy for E-Safety and the Acceptable use of ICT, the Internet and Personal Data

Ratified: January 2018
Review: January 2019

## 1 Introduction

This policy has been developed from the Internet Access and Ethics Policy which was written in Summer/Autumn 2000 by a staff group chaired by the ICT Co-ordinator. It refers to the school's curriculum ICT Policy, Anti-bullying Policy and our pupils' Code of Practice, which is displayed in classrooms, and the staff Code of Practice, which is included in the Staff Handbook. It takes account of Cambridgeshire's Internet Safety Guidance and Data Protection Legislation. It was updated in September 2003, February 2008 and December 2012 in order to incorporate guidance on current issues, for example handling personal data. The latest update was in December 2017.

Due to the fast changing nature of ICT and particularly safety on the internet, this policy will be reviewed bi-annually by the Leadership Team and be part of the Governors' regular review cycle.

The policy outlines what Girton Glebe believes are the most appropriate ways for pupils and staff to use computer hardware and software, including electronic mail and the world-wide web including learning platforms.

It explains how Girton Glebe strives to meet legal and moral responsibilities.

## 2 Aims and Values

At Girton Glebe Primary School, we encourage individual achievement alongside consideration for the needs of others. We ensure that the children are supported in a safe and secure learning environment where security measures are balanced appropriately through the use of our Code of Practice. These guidelines for pupils are on display in each classroom and are discussed at an appropriate level with each cohort.

Our aim is to provide a balanced approach to the use of technology through cross-curricular projects and explicit E-Safety teaching. Within the curriculum, children are encouraged to explore the benefits of all relevant technology and evaluate their use of Computing.
Applying skills to real life situations, our children will become equipped with the knowledge and ability required to use a wide variety of technology appropriately and responsibly.

By maintaining a high profile of the risks associated with technology our children are equipped at home and at school with the knowledge and ability to deal with technology safely. All members of our school community recognise the need and importance for an e-Safety policy and to adhere to it.

See Appendix 1 – Code of Practice for Pupil ICT Use

## 3 E-Safety Champion

Girton Glebe Primary School has an appointed E-Safety Champion who is the main point of contact for E-Safety related issues and incidents. The E-Safety Champion will always be a Designated Person for Child Protection.
The duties of the E-Safety Champion include:

- Having operational responsibility for ensuring the development, maintenance and review of the school's eSafety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- Ensuring all staff are aware of reporting procedures and requirements should an eSafety incident occur.
- Ensuring an eSafety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally up-to-date with eSafety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Providing or arranging eSafety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, children and governors are updated as necessary.
- Liaising closely with the school's Designated Senior Person / Child Protection Officer to ensure a co-ordinated approach across relevant safeguarding areas.

## 4 Online Work

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.

### 4.1 Internet Access

Internet access will provide effective learning for children by:

- teachers setting clear objectives 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;
- staff bookmarking approved sites.

### 4.2 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 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.

#### 4.2.1 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

### 4.3 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 Virtual Learning Environment LP+ (Learning Platform +) will have access to individual internal email.

Public real-time chat, such as AIM, Google Talk or Windows Live Messenger, 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;
- school e-mail addresses for pupils will not identify pupils. First or last names must not appear in pupil email addresses;
- local internet forums will be closely supervised by the class teacher;
- pupils will be taught how to safely manage their e-mail address.

### 4.4 Web Publishing

When publishing material on the world-wide web:

- 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 only will be used on the web site – 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;
- photographs of pupils may be published, but where a photograph is used, children are not identified by name. Parents have the option of withholding consent for their child's photograph to appear on the internet. Parents are informed of this policy on their child's admission through the 'New Parents Pack' and it is their responsibility to inform the school of such a request.

See Appendix 2 – Guidelines for Publishing in the Community

### 4.5 Virtual Learning Environments (VLEs)

Virtual Learning Environments provide a secure online environment in which children can work and collaborate.

The following guidance should be followed when using a VLE:

- The learning platform does enable open communication between children within the Girton Glebe community via class forums and personal emails. Pupils are not visible to anyone outside the school community and all use email addresses are hidden.
- Children must be familiar with the Code of Conduct for using a VLE given in Appendix 4. Pupils must be reminded regularly about the Code of Conduct and are taught to report to teachers about any content that upsets them
- Staff must take particular care to maintain a protective ethos when communicating with children within the VLE. The Headteacher and Computing subject leader will monitor the comments and communications made within the VLE 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 courses they manage to ensure appropriate use.

### 4.6 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.

### 4.7 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 web-based 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.

### 4.8 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 encouraged 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

### 4.9 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.

## 5 Internet Safety

Internet access is a necessary part of the statutory curriculum. It is an entitlement for pupils based on responsible use. At Girton Glebe 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.

### 5.1 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 via links saved on the school intranet, via a direct link on the class page of the school learning platform or via an app.

- at Key Stage 2, pupils will continue to work from links via the school intranet and will also be introduced to conducting online searches. In Year 5 and 6 the children are also taught to discriminate between the validity of their results.

### 5.2 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 international 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 (Appendix 1)
- an annual review of responsible Internet use both at school and home as part of the Computing 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.

## 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 ICT 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, NAA 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, eg Target Tracker
- File encryption when transferring data outside secure networks, eg to/from the NHS

### 6.1 User Profiles

All IT users at Girton Glebe 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 longer periods of time. They must ensure that passwords are not saved on their computer, including their Parentmail log-on.

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-level data in the file, eg planning, worksheets, etc
- Encryption is required when:
    - transferring pupil-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 Girton Glebe 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 ICT 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. 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 ICT subject leader.

- Teachers may use school laptops for e-mail and internet access. However they should follow the guidance set out in 'Acceptable ICT 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 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 phone bills etc. are the responsibility of the user.

### 6.5 Use of Cloud-Based Storage

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

- Target Tracker provides online access to pupil-level assessment data
- Micro Librarian Systems provides online access to library records
- The school website hosts planning and teaching resources
- Dropbox 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, eg the Target Tracker system. 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, assessments on Target Tracker, 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.

## 7 Mobile Phones

Pupils should not bring mobile phones in to school. If this is unavoidable, they must be handed in to the school office on arrival and collected on departure. Staff members must ensure that mobile phones are stored securely and not used in front of children. If staff mobile phones are stored in an unsecured place which children could access, e.g. an unlocked drawer in a classroom, they should be password protected. Staff must never take photos on mobile phones.

## 8 Cameras

School cameras or i-pads should be for taking school photographs. Photos should be uploaded to laptops at the earliest opportunity and deleted from cameras when uploaded. If use of a personal camera is unavoidable, photos should be uploaded immediately upon return to school and deleted before the camera leaves school premises. Parents should only take photos of their own children at school events. Any photos taken by parents at school events should not be published online including social media.

## 9 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.

## 10 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.

Parents and pupils will need to work in partnership with staff to resolve issues.

## 11 Monitoring and Review

The ICT Subject Leader and the Headteacher are responsible for checking that the policy is being implemented on a day-to-day basis, and discussing its effectiveness regularly.

This policy will be reviewed as part of the Governors' usual review cycle.

**Appendix 1a – Code of Practice for Pupils in EYFS**

## Code of Practice for Pupils in EYFS

The school has computers to help us learn.
These rules will keep everyone safe:

- I will only use websites that my teacher has set up for me.
- I will check with my teacher before using the internet.
- I will tell my teacher if I see something on the computer that worries or upsets me.

**Appendix 1b – Code of Practice for Pupils in Key Stage 1**

## Code of Practice for Pupils in Key Stage 1

The school has computers to help us learn.
These rules will keep everyone safe:

- I will keep my logins and passwords secret
- I will not use anyone else's files or logins.
- I will check with my teacher before using the internet.
- I will only use the computer for things my teacher has agreed to.
- I will tell my teacher if I see something on the computer that worries or upsets me.
- I will not bring in memory sticks

## Appendix 1c – Code of Practice for Pupils in Key Stage 2

## Code of Practice for Pupils in Key Stage 2

The school has installed computers and internet access to help our learning.

These rules will keep everyone safe and help us to be fair to others:

- I will keep my logins and passwords private.
- I will not open other people's files **or use other people's logins**
- I will only use the computers and ICT equipment for activities when approved by and supervised by a responsible adult.
- I will not bring in memory sticks or portable storage devices.
- If I bring in a mobile phone it will be stored in the school office.
- I will ask permission from a member of staff before using the internet.
- I will only message people I know or my teacher has approved.
- The messages I send will be polite and responsible.
- I will not give my home address, telephone number or email address to anyone online or arrange to meet someone I have met online.
- I will report any unpleasant material or messages sent to me.
- I understand that the school may check my computer files and may monitor the internet sites I visit and messages I send and receive.

## 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:

- Newsletters
- Twitter
- *the whiteboard*
- School Website
- Girton Parish News
- School Prospectus
- letters to parents
- information leaflets for parents

Pupils are identified by first name and class or year group, rather than by their full name. 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 children are not identified by name if a photograph is used. Parents have the option of withholding consent for their child's photograph to appear on the internet. This applies to editions of school newsletter, Twitter, Girton Parish News, the school prospectus and *the whiteboard* which are all reproduced online. Parents are informed of their right to withdraw consent for their child's photo to appear online at the time of their child's admission through the 'New Parents Pack' and it is their responsibility to inform the school of such a request.

**Publishing to the Wider Community**

Including:

- In touch
- Local Newspapers

Photographs of pupils may be published, having first obtained parental permission. In general they should not identify a child by 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.
When attending trips or visits, permission to take photographs by external agencies will not be given unless permission has been sought and given by parents in advance.

## Appendix 3 – Acceptable ICT Use Statement for Staff

### Acceptable ICT 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 ICT, 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 ICT Use Statement and return it to office for inclusion on the Single Central Record.

**General Use of ICT:**

- Use of the school's ICT equipment, (including laptops, 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.
- Supply teachers must log on using supply user name only and staff members must not share personal logs on with supply staff.
- Any activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.
- Users are responsible for all e-mails sent and for contacts made that may result in e-mails being received.
- Copyright of materials must be respected.
- Staff are not encouraged to be in direct email contact with parents, unless there are exceptional circumstances which would be discussed with the

headteacher. Parents will be directed to use the office email if email contact is required.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Staff should remember that their conduct on social media should be in keeping with the professional standards and that disciplinary action may be taken if this is not adhered to.

**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) can be saved on staff share or within staff member's 'My Documents' folder. 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

**Use of 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 courses that you teach in 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 my profile.