St. Patrick's Catholic Primary School E-Safety Policy

October 2020
Review October 2023

St. Patrick′s Catholic Primary School

We strive for excellence within a caring and diverse community, nurturing the Catholic faith, respecting each other, living, working and growing together as part of God′s family.

E-Safety Policy: The Acceptable Use of the Internet and Related Technologies

The internet and other digital technologies permeate all aspects of life in a modern technological society. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

'To use these new technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both inside and outside the classroom'
(DFES, eStrategy 2005)

The Green Paper *Every Child Matters* and the provisions of the *Children Act 2004*, *Working Together to Safeguard Children* sets out how organisations and individuals should work together to safeguard and promote the welfare of children.

The ′staying safe′ outcome includes aims that children and young people are:

- *Safe from maltreatment, neglect, violence and sexual exploitation*
- *Safe from radicalisation*
- *Safe from accidental injury and death*
- *Safe from bullying and discrimination*
- *Safe from crime and anti-social behaviour in and out of school*
- *Secure stable and cared for*

Much of these aims apply equally to the 'virtual world' that children and young people encounter whenever they use ICT in its various forms. For example, we know that the internet has been used for grooming children and young people with the ultimate aim of exploiting them sexually; we know that ICT can offer new weapons for bullies, who may torment their victims via websites or text messages; and we know that children and young people have been exposed to inappropriate content when online, which can sometimes lead to their involvement in crime and anti-social behaviour.

It is the duty of St Patrick's that every child in our school is safe and the same principals should apply to the 'virtual' or digital world as would be applied to the school's physical buildings.

This document is drawn up to protect all parties - the children, the staff and the school. It aims to provide clear advice and guidance on how to minimise risks and how to deal with infringements.

1. The Technologies

ICT in the 21st century has an all-encompassing role within the lives of children and adults. New technologies enhance communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
- E-mail
- Instant messaging often using web cams
- Blogs (an on-line interactive diary)
- Podcasting (radio/audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat rooms
- Gaming sites
- Music download sites
- Mobile phones and devices with cameras and video functionality
- Mobile phones and devices with e-mail and web functionality

2. Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-Safety education programme for pupils, staff and parents.

3. Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to imbed safe practices into the culture of the

school. The Head Teacher ensures that the Policy is implemented and compliance with the Policy is monitored. The responsibility for e-safety has been designated to a member of the senior management team.

Our school e-Safety Coordinators are: The ICT Coordinator and Head Teacher

The e-Safety Coordinators ensure they keep up to date with e-Safety issues and guidance through liaison with the LEA, DfES and through organisations such The Child Exploitation and Online Protection (CEOP). The school's e-Safety coordinators ensure that all senior leadership, staff and Governors are updated as necessary.

Governors need to have an overview understanding of e-Safety issues and strategies at this school. St Patrick's ensure our governors are aware of local and national guidance on e-safety and are updated on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following e-Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate behaviour.

4. How will complaints regarding e-Safety be handled?

The school will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview/counselling by an e-Safety Coordinator
- Informing parents or carers
- Removal of Internet or computer access for a period
- Referral to LEA / Police

Our ICT Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head Teacher.

Complaints of cyber bullying are dealt with in accordance with our Positive Behaviour Policy. Complaints related to child protection, radicalisation or extremism are dealt with in accordance with our Safeguarding Policy.

Managing the Internet Safely

Why is Internet access important?

The Internet is an essential element in 21st century life for education, business and social interaction. ICT skills and knowledge are vital to access life-long learning and employment; indeed ICT is now seen as a functional, essential life-skill along with English and mathematics. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using technology including the Internet. All pupils should be taught to use the Internet efficiently and safely, and to develop a responsible and mature approach to accessing and interpreting information. The Internet can benefit the professional work of staff and enhances the school's management information and business administration systems.

The risks

The Internet is an open communications channel, available to all. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it both an invaluable resource used by millions of people every day, as well as a potential risk to young and vulnerable people.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, extremism, crime and racism that would be considered wholly inappropriate and restricted elsewhere.

The filtering systems used in our school block inappropriate content, including extremist content. We also filter out social media, such as Facebook and Twitter, and prevent further access to unsafe sites or information that are unblocked when first found. User activity can be investigated and the ICT Technician and school staff will alert Senior Management as soon as there are safety concerns, or a user has breached the ICT Acceptable Use Policy.

Where staff, students or visitors find unblocked extremist or other internet content that is inappropriate they must report it to the ICT Coordinator or a member of Senior Management immediately.

In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and to teach pupils to be aware of, and respond responsibly to, any risk. This must be within a 'No Blame', supportive culture if pupils are to report abuse.

This school:

- Maintains broadband connectivity through Virgin
- Works in partnership with the LEA to ensure any concerns about the system are communicated to AdEPT Education (formerly Atomwide) and LGfL so that systems remain robust and protect students

- Ensures network health through appropriate anti-virus software etc and network set-up so staff and pupils cannot download executable files such as .exe / .com / .vbs etc
- Ensures our network is 'healthy' by carrying out automated anti-virus scans on a daily basis using Sophos
- Ensures the Systems Administrator / Network Manager is up-to-date with LEA/National services and policies
- Ensures the Systems Administrator / Network Manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately
- Never allows pupils access to Internet logs
- Uses log-ins for pupils that progressively teach children the finer points of password security and data protection as they go through the school (ie. *first names in Reception, first names and generic password in Year 1 – moving through to Year 6 where they will use a first.surname login and case sensitive password created by each student and only known by them*)
- Never sends personal data over the Internet unless it is encrypted or otherwise secured through Egress Switch
- Uses 'safer' search engines with pupils and activates 'safe' search where appropriate
- Ensures pupils only publish within appropriately secure learning environment
- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access
- Uses the AdEPT Education filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature
- Staff preview all sites before use [where not previously viewed] or only use sites accessed from managed 'safe' environments
- Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required
- Is vigilant when conducting 'raw' image search with pupils eg. Google image search
- Informs users that Internet use is monitored
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Coordinator. Our Systems Administrator report to Atomwide/LGfL where necessary
- Blocks all chat rooms and social networking sites
- Only uses approved blogging or discussion sites
- Has blocked pupil access to music download or shopping sites
- Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an Acceptable Use Policy (please see Appendix 1 and 2) which is fully explained and used as part of the teaching programme

- Requires all staff to sign an Acceptable Use Policy (please see Appendix 2), which is part of their induction process, and keeps a copy on file
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme
- Keeps a record, eg. details of any onsite or offsite bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour policy
- Makes information for reporting offensive materials, abuse, bullying, etc available for pupils, staff and parents (please see the school Safeguarding Policy)
- Immediately refers any material we suspect is illegal to the appropriate authorities – LEA / Police
- Fosters a 'No Blame' environment that encourages pupils to tell a teacher or responsible adult immediately if they encounter any material that makes them feel uncomfortable
- Ensures pupils and staff know what to do if they find inappropriate web material (*ie. to switch off the monitor and report the URL to the teacher or System Manager*)
- Ensures pupils and staff know what to do if there is a cyber-bullying incident
- Has a clear, progressive e-Safety education programme throughout all Key Stages, built on LEA / London / national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

    - To STOP and THINK before they CLICK
    - To expect a wider range of content, both in level and in audience, than is found in the school library or on TV
    - To discriminate between fact, fiction and opinion
    - To develop a range of strategies to validate and verify information before accepting its accuracy
    - To skim and scan information
    - To be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - To know some search engines / web sites that are more likely to bring effective results
    - To know how to narrow down or refine a search
    - To understand how search engines work [for older pupils]
    - To understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - To understand 'Netiquette' behaviour when using an online environment such as a chat / discussion forum, (*ie. No bad language, propositions, or other inappropriate behavior*)
    - To not download any files – such as music files - without permission
    - To understand why they should <u>not</u> post or share detailed accounts of their personal lives, contact information, daily routines, photographs and videos
    - To have strategies for dealing with receipt of inappropriate materials

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights

- Makes training available annually to staff on the e-safety education program

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Information in leaflets; school newsletters; and on the school web site
    - Demonstrations, practical sessions held at school
    - Suggestions for safe internet use at home
    - Provision of information about national support sites for parents.

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our school and increasingly for pupils and homes. Directed e-mail use in schools can bring significant educational benefits through increased ease of communication between students and staff, or within local and international school projects.

However, unregulated e-mail can provide a means of access to a pupil that bypasses the traditional school physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

This school:

- Does not publish personal e-mail addresses of pupils or staff on the school website
- If one of our staff or pupils receives an e-mail that we consider is particularly disturbing, or breaks the law, we contact the police
- Accounts are managed effectively, with up to date account details of users

Pupils:

- We only use LGfL Safe mail with pupils

- Pupils can only use the school e-mail accounts on the school system

- Pupils are introduced to, and use, e-mail as part of the ICT scheme of work from Key Stage 2

- Pupils are taught about the safety and ′netiquette′ of using e-mail:
    - Not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer
    - That an e-mail is a form of publishing where the message should be clear, short and concise

- That any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc
- To 'stop and think before they click' and not open attachments unless they are sure the source is safe
- The sending of attachments should be limited
- Embedding adverts is not allowed
- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature
- Not to respond to malicious or threatening messages
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them
- That forwarding 'chain' e-mail letters is not permitted

- Pupils sign the Acceptable Use Policy to say they have read and understood the e-Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff use the LGfL e-mail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to an external organisation is written carefully (and may require authorisation) in the same way as a letter written on school headed paper. It should follow the school 'house-style':
  - The sending of attachments should be limited
  - The sending of chain letters is not permitted
  - Embedding adverts is not allowed

- Staff read and sign the appropriate Acceptable Use Policy to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Using digital images and video safely

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for

information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety. A senior member of staff needs to oversee and authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website.

In this school:

- The Headteacher and Deputy Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained
- Uploading of information is restricted to the school's administration officers / ICT Technician / subject leaders / teachers in their class areas
- The school web site complies with the school's guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published

Use of still and moving images

Most importantly, care should always be taken when using photographs or video footage of pupils on the school website. This reduces the risk of inappropriate, unsolicited attention from people outside the school.

An easy rule to remember is: *If the pupil is named, avoid using their photograph / video footage. If the photograph / video is used, avoid naming the pupil.*

When using still and moving images this school ensures:

- Group photographs are used where possible, rather than photos of individual children
- Pupils are in suitable dress to reduce the risk of inappropriate use
- Photographs published on the web do not have names attached
- We gain parental / carer permission for use of digital photographs or video involving their child, as part of the school agreement form when their daughter / son joins the school
- Digital images / video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs

- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils
- Pupils are only able to publish to their own 'safe' web-portal on the LGfL website in school
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work

Using the school network, equipment and data safely:

General guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system, or to monitor any Internet or email activity on the network.

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-Safety and Acceptable Use Policy. Following this, they are set-up with Internet and email access and can be given an individual network log-in (username and password)
- Makes it clear that staff must keep their log-in username and password private and must not leave them where others can find them.
- Creates temporary logins for supply teachers and external guests that are not directly employed by the school
- Makes clear that pupils should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network
- Makes clear that no one should log on as another user – if two people log-on at the same time this may corrupt personal files and profiles
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off or lock their computer when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and they switch off the whiteboards when not in use

- Has set-up the network so that users cannot download harmful executable files / programmes
- Has blocked access to music download or shopping sites – except those approved for educational purposes
- Scans all mobile equipment with anti-virus and spyware software before it is connected to the network
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any significant personal use as defined by HM Revenue & Customs
- Makes clear that staff accessing LEA systems do so in accordance with any Corporate policies
- Maintains equipment to ensure Health and Safety is followed
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role
- Does not allow any outside agencies to access the network remotely except where there is a clear professional need and then access is restricted and is only through approved systems
- Follows LEA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network
- Reviews the school ICT systems regularly with regard to security

School emails

School emails are subject to Freedom of Information requests, and as such the email service provided by the school is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. While working at St Patrick's School any staff′s school email address ending with @st-patricks.waltham.sch.uk may be accessed at any time and without notice if the management team needs to access any information or feels that you may be in breach of The Data Protection Act or the school′s Acceptable Use Policy.

YouTube

When using YouTube in the classroom, all staff must adhere to the following:

- Be logged in to YouTube at all times, using the school login account, to ensure the safety feature is enabled
- Always screen/check the entire footage of any YouTube material before using it in the classroom and never blindly click on a link without first screening the said material
- Always ensure that any visible links do not contain inappropriate material. If unsure, freeze the projector with YouTube minimised then do a visual check on the PC monitor
- Members of staff are responsible for providing safe and secure educational experiences to children and may face disciplinary action for exposing children to any inappropriate material

Virtual Lessons or Meetings (Live and Recorded)

When hosting an online meeting or teaching a live or recorded session for children or adults, staff should ensure that the following points are considered:

- The virtual server should have suitable security in place and those hosting the meeting should ensure they can end the meeting if needed
- Staff should use school devices and networks to hold meetings or classes where possible, to ensure that the school′s filtering and monitoring software is actively used
- Any displays, photos or artwork that are on display in the background should be carefully considered and ideally nondescript
- Staff, parents and pupils should only partake in virtual meets that are held in living or communal areas (bedrooms or bathrooms are not suitable)
- All visual participants should be suitably dressed in appropriate attire for the entire virtual meeting or class

Useful resources

Chat Danger
www.chatdanger.com/
Child Exploitation and Online Protection Centre
www.ceop.gov.uk/
Childnet
www.childnet-int.org/
Digizen
www.digizen.org/
Think U Know
www.thinkuknow.co.uk/
UK Council for Child Internet Safety
www.dfes.gov.uk/byronreview/

Appendix 1

ST. PATRICK'S CATHOLIC PRIMARY SCHOOL

KS1 ICT ACCEPTABLE USE POLICY

I promise:

- ✓ I will treat all school equipment with care and respect
- ✓ I will only open, edit and delete my own files
- ✓ I will only use the Internet when supervised by an adult
- ✓ I will only click on icons and links when I am told to by the teacher and I know they are safe
- ✓ If I see something I don't like on a screen, I will always tell an adult
- ✓ I understand that these rules are to keep me safe
- ✓ Most importantly I will remember that if I am unsure about anything, I should ask or tell a teacher

I have read and understood this policy and agree to follow it.

Name: _____ Class: _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the Internet.

Parent/Carer Signature: _____ Date: _____

Appendix 2

ST. PATRICK'S CATHOLIC PRIMARY SCHOOL

KS2 ICT ACCEPTABLE USE POLICY

- I will only use ICT in school for school purposes and will treat all school equipment with care and respect
- I will only use my school e-mail address when e-mailing and will only open attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not deliberately look for, download, upload, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately
- I will not give out my own or others details such as name, phone number or home address
- I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not install any program nor change the settings of any program or equipment unless directed by a teacher or member of staff
- I will check that information I use from the Internet is from a trusted site and reference any work or materials I use that are not my own
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- Most importantly I will remember that if I am in doubt about anything, I should ask a teacher

I have read and understood this policy and agree to follow it.

Name: _____ Class: _____

I have read and discussed this policy with my child and give permission for him/her to use the school's ICT systems, including the Internet.

Parent/Carer Signature: _____ Date: _____

Acceptable Use Policy (AUP): Staff agreement form

Covers use of digital technologies in school: ie. email, Internet, intranet and network resources, learning platform, software, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal or share my password(s) to anyone or allow students to log into systems under my own account
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system(s) for any school business. (This is currently LGfL Staffmail)
- I will only use the approved school email, school Learning Platform or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the school' ICT Technician and e-Safety Coordinators.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not publish or distribute work that is protected by copyright.
- I will not connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff **without prior permission** and will not store images at home **without permission**.
- I will use the school's Learning Platform in accordance with school protocols.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities

- I will access school resources remotely (such as from home) only through the LGfL / school approved methods and follow e-security protocols to access and interact with those materials.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols and good practice when using any such data at any location.
- I understand that the school policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's e-safety curriculum into my teaching.
- I will alert the school's named child protection officer, or a relevant member of the safeguarding team, if I feel the behaviour of any child I teach may be a cause for concern.
- I will only use LA systems in accordance with any corporate policies.
- I understand that all Internet usage and network usage (including emails) can be logged and this information could be made available to my manager on request.
- I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to the school's Headteacher or a relevant member of the safeguarding team
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I agree to abide by all the points above. I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-Safety policies.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

Authorised Signature (Headteacher)

I approve this user to be set-up.

Signature ..... Date .....