****

**Policy Data Sheet**

|  |  |
| --- | --- |
| **Policy Name:** | Big Life Schools E-Safety Policy  |
| **Document Reference:**  | BLSch |
| **Version Number:**  | 1 |
| **Ratified By Head Teacher:**  | N/A |
| **Chair of Governing Body Ratified Date:**  | N/A |
| **Board approval needed?** | MAT  |
| **Board Ratified Date:**  | 16/7/19 |
| **Review Period:** | 3 years  |
| **Review Date:**  | Under Review  |

**Contents**

[**1. Rationale 2**](#_Toc23156686)

[**2. Scope of the Policy 2**](#_Toc23156687)

[**3. Roles and Responsibilities 2**](#_Toc23156688)

[**4. E-safety risks and strategies to minimise risk 4**](#_Toc23156689)

[**5. Acceptable use of ICT 4**](#_Toc23156690)

[**6. Unacceptable Use of ICT 6**](#_Toc23156691)

[**7. Reporting Procedures 7**](#_Toc23156692)

[**8. Associated Policies 8**](#_Toc23156693)

[**9. Useful Links – E Safety information and support 8**](#_Toc23156694)

[**10. Related Legislation 8**](#_Toc23156695)

# **Rationale**

Big Life Schools recognises the importance of relevant and new technologies in the lives of our pupils. The internet and other digital information technologies are powerful tools, which can open up new and exciting opportunities for learning. Internet use is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement for every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. (Article 13 – Right to information)

# **Scope of the Policy**

This policy applies to all members of Longsight and Unity Community Primary School (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of Unity Community Primary School systems, both in and out of our school. It is the duty of everyone to ensure that children are;

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

This is relevant to the virtual world just as much as the physical world in which our children live. Children and young people may encounter dangers whenever they use ICT. Our pupils are taught about the risks they face online and how to limit them; these risks include, but are not limited to, fraud, malicious software, identity theft, bullying, grooming, stalking, abusive behaviours and radicalisation. It is the duty of the school and all of its staff to ensure that every child in our care is safe when using technology.

It is, however, equally important to recognise that technology, in particular the internet, is one of the most powerful learning resources available today. When it is properly used, the internet, can broaden the horizons of children and help prepare them for the wider world.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

Both Longsight and Unity will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

# **Roles and Responsibilities**

The following section outlines the e-safety roles and responsibilities of individuals and groups within Unity Community Primary School.

1. **Governors**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Safeguarding Governor will oversee e-safety in the school. The role of the e-Safety Governor will include:

* Regular meetings with the IT lead/Designated Safeguarding Lead.
* Regular monitoring of e-safety incident logs.
* Reporting to the Local Governing Body
1. **Headteacher and Senior Leaders**
* The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
* The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see NSPCC flow chart on dealing with e-safety incidents.)
* The Headteacher/Senior Leadership Team are responsible for ensuring that the Computing Co-ordinator/ Designated Safeguarding Leads and other relevant staff receive suitable training to enable them to carry out their e-safety roles.
* The Headteacher/Senior Leadership Team will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.
* The Senior Leadership Team will receive regular monitoring reports from the DSL lead.
1. **Designated Safeguarding Leads**
* Leads on e-safety issues.
* Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents.
* Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
* Attends relevant training, disseminating to all staff, including;
	+ Sharing of personal data.
	+ Accessing illegal/inappropriate materials.
	+ Contacting inappropriate adults/strangers on-line.
	+ Potential or actual incidents of grooming.
	+ Cyber-bullying.
	+ Peer on peer related incidents on and offline.
* Liaises with the Local Authority/relevant body.
* Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
* Liaises with EE regarding any e-safety issues and use of school systems.
* Review incident logs and filtering/change control logs.
* Attends relevant meeting/committee of Governors.
* Reports regularly to Senior Leadership Team.
1. **Network Support**

MGL are responsible for ensuring:

* That the school’s technical infrastructure is secure and is not open to misuse or malicious attack.
* That the school meets required e-safety technical requirements and any Local Authority/other relevant body E-Safety Policy/Guidance that may apply.
* That users may only access the networks and devices through a properly enforced password protection policy.
* That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
* That the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher/E-Safety Manager/ Co-ordinator/ Designated Safeguarding Lead for investigation/action/sanction.
* That monitoring software/systems are implemented and updated as agreed in school policies.
1. **Teaching and Support Staff**

Teaching and Support Staff are responsible for ensuring that:

* They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
* They have read and understood The Big Life Groups IT, internet and social media policy in addition to the group’s mobile phone policy.
* They report any suspected misuse or problem to the Headteacher/DSL for investigation/action/sanction.
* All digital communications with students/parents/carers should be on a professional level and only carried out using official school systems.
* E-safety issues are embedded in all aspects of the curriculum and other activities.
* Pupils understand and follow the e-safety and acceptable use agreements.
* Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
* They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices.
* In lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

# **E-safety risks and strategies to minimise risk**

1. Risks

The risks can be summarised under the following headings:

1. Exposure to age-inappropriate material.
2. Exposure to inaccurate or misleading information.
3. Exposure to socially unacceptable material such as that inciting violence, hate or intolerance.
4. Exposure to illegal material such as images of child abuse.
5. Grooming using communication technologies, leading to sexual assault and/or child prostitution.
6. Exposure of minors to inappropriate commercial advertising.
7. Exposure to online gambling services.
8. Commercial or financial scams.
9. Bullying via websites, mobile phones or other forms of communication device.
10. Downloading copyrighted materials e.g. films and music.
11. Excessive amounts of ‘screen-time.’
12. Exposure to material supporting terrorism or extremism.
13. **Strategies to minimise risk**

As a school, it is our duty of care alongside that of staff, parents/carers and other members of the community to protect our children and young people from these dangers. This can be achieved by many different mechanisms working together;

* E-safety education as part of the day to day curriculum, including pupils understanding the importance of reporting abuse, misuse or access to inappropriate materials and knowing how to do so.
* A signed Acceptable Use Agreement between the school, pupils, parent/carers and community users.
* Pupils should be helped to understand the need for the agreement and encouraged to adopt safe and responsible use, both within and outside school.
* All parents/carers consent for web publication of work and photographs.
* E-safety support to be given to parents/carers e.g. parent/carer information sessions, information available on the school website.
* Parents/carers to be made aware of the school E-safety Policy.
* Internet filtering programmes that screen all internet traffic coming into/going out of the school (EE filtering systems.)
* Age appropriate e-safety rules displayed in all classrooms.
* E-bullying to be addressed during anti-bullying week and at other times of the year.
* Safeguarding issues and e-safety concerns to be reported to a Designated Safeguarding Lead
* The use of all technologies to be monitored by all staff.
* All staff/volunteers to sign and follow the Big Life IT, Email and Social Networking Policy.
* Staff/volunteers to complete e-safety training.
* All staff/volunteers to report any e-safety issues/concerns to a Designated Safeguarding Lead.
* Governors to be aware of e-safety issues and to be given regular updates on any e-safety concerns.

# **Acceptable use of ICT**

All staff, pupils, visitors and community users within the school are expected to behave in a responsible manner when using ICT equipment and behave in ways which minimise the risk of exposure to inappropriate materials and harm to themselves and others. Staff must ensure that all sensitive data is stored in a manner which is in keeping with the General Data Protection Regulation 2018 (GDPR). Appendix 1, 2 and 3 will be used to inform users of ICT in school of our acceptable user agreements.

1. **Current Technologies**

ICT provides many essential tools for modern education and the internet is an invaluable resource for learning. For this reason we must simultaneously embrace new technologies, whilst being vigilant against the risks presented by these technologies to the children in our care. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and outside of school include;

* The internet.
* Browsing.
* Email.
* Instant messaging often using webcams.
* Blogs (an online interactive diary.)
* Podcasting (radio/audio broadcasts downloaded to a computer or MP3/4 player.)
* Social networking sites (Facebook, Instagram, Twitter, Snapchat etc.)
* Video broadcasting sites.
* Chat rooms.
* Gaming sites.
* Music download sites.
* Mobile phones with internet, cameras and video functionality.
* Mobile technology that is interment ready (games consoles, tablets.)

**Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
* In accordance with guidance from the Information Commissioner’s Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
* Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
* Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
* Pupils must not take, use, share, publish or distribute images of others without their permission.
* Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
* Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or social network sites.
* Written permission from parents or carers will be obtained before photographs of pupils are published external websites or promotional material.
* Pupil’s work can only be published with the permission of the pupil and parents or carers.

Further to this, the following table shows how our school currently considers using these technologies for education.

|  |  |  |
| --- | --- | --- |
|  | **Staff & Other Adults** | **Students** |
| **Communication****Technologies** | **Allowed** | **Allowed at certain times (breaks & lunchtime)** | **Selected staff only** | **Not** **Allowed** | **Not** **Allowed** | **Allowed** | **Allowed at certain times** | **Allowed with staff permission** |
| **Mobile phones may be brought into schools** | ü |  |  |  | ü |  |  |  |
| **Use of mobile phones in lessons** |  |  |  | ü | ü |  |  |  |
| **Use of mobile phones in social times** | ü |  |  |  | ü |  |  |  |
| **Taking photos on school mobile phones** | ü |  | ] |  | N/A |  |  |  |
| **Taking photos on personal mobile phones** |  |  | ] | ü | ü |  |  |  |
| **Taking photos on school camera (projects/staff/students)** | ü |  |  |  |  |  |  | ü |
| **Use of other mobile devices (tablets)****(projects/staff/students)** | ü |  |  |  |  |  |  | ü |
| **Use of personal e mail address in school or on school network** |  | ü |  |  | ü |  |  |  |
| **Use of school e mail for personal e mail** |  | ü |  |  | ü |  |  |  |
| **Use of messaging apps (in school time)** |  | ü |  |  | ü |  |  |  |
| **Use of social any media (in school time)** |  | ü |  |  | ü |  |  |  |
| **Use of blogs (in school time)** |  | ü |  |  | ü |  |  |  |

# **Unacceptable Use of ICT**

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

|  |
| --- |
| **Users shall not visit internet sites, make, post, download, upload, data transfer, communicate, pass on, materials, remarks, proposals or comments that contain or relate to:** |
| **USER ACTIONS** | **Acceptable** | **Acceptable****at certain times** | **Acceptable for nominated users** | **Unacceptable** | **Unacceptable and illegal** |
| **Child sexual abuse images – The making, production or distribution of indecent images of children, contrary to the Protection of Children Act 1978.** |  |  |  |  | ü |
| **Grooming, incitement, arrangement or facilitation of sexual acts of children, contrary to the Sexual Offences Act 2003.** |  |  |  |  | ü |
| **Possession of an extreme pornographic image (grossly offensive, or of an obscene character), contrary to the Criminal Justice and Immigration Act 2008.** |  |  |  |  | ü |
| **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation), contrary to the Public Order Act 1986.** |  |  |  |  | ü |
| **Pornography** |  |  |  | ü |  |
| **Promotion of any kind of discrimination** |  |  |  |  | ü |
| **Threatening behaviour, including promotion of physical violence or mental harm** |  |  |  |  | ü |
| **Any other information which may be offensive to colleagues or breaches of the integrity of the ethos of the school or brings the school into disrepute.** |  |  |  | ü |  |
| **Using school systems to run a private business** |  |  |  | ü |  |
| **Using systems, application, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy/college** |  |  |  | ü |  |
| **Infringing copyright** |  |  |  | ü |  |
| **Revealing or publicising confidential or proprietary information (e.g. financial personal information, databases, computer / network access codes and passwords).** |  |  |  | ü |  |
| **Creating or propagating computer viruses or other harmful files** |  |  |  | ü |  |
| **Unfair usage (downloading / uploading large files that hinders others in their use of the internet).** |  |  |  | ü |  |
| **Online Gaming (educational)** |  | ü |  |  |  |
| **Online Gaming (non-educational)** |  |  |  | ü |  |
| **Online gambling** |  |  |  | ü |  |
| **Online shopping/commerce** |  | ü |  |  |  |
| **File sharing** |  |  | ü |  |  |
| **Use of Social Media** |  | ü |  |  |  |
| **Use of messaging apps** |  | ü |  |  |  |

# **Reporting Procedures**

1. **Staff or Volunteers**

If a member of staff, volunteer is believed to have misused the internet or learning platform the issue will be investigated in line with The Big Life Groups disciplinary procedure. All instances must be reported to the Headteacher and HR with immediate effect. In instances where safeguarding is a concern the Group Safeguarding Lead must be notified.

1. **Community**

If a community member is reported to have used the internet inappropriately the incident will be investigated in line with The Big Life Groups Incident and Serious Incident Requiring investigation Policy. If the incident is of a safeguarding concern the Group safeguarding lead must be notified immediately.

1. **Pupils**

Should a pupil be found to misuse the online facilities whilst at school, staff should report this to a Designated Safeguarding Lead or Senior Leader immediately.

The following local procedures will also apply;

* Pupils found to be misusing the internet by not following the Acceptable Use Agreement may have a letter sent home to parents/carers explaining the reason for suspending the pupil’s use for a particular lesson or activity
* Further misuse of the agreement may result in further sanctions which could include not being allowed to access the internet for a period of time
* A letter may be sent to parents/carers outlining the breach in Safeguarding Policy where a pupil is deemed to have misused technology against another pupil or adult
* In the event that a pupil accidentally accesses inappropriate materials the pupil should report this to a member of staff immediately and take appropriate action to hide the screen or close the window, so that the staff member can take the appropriate action. Where a pupil feels unable to disclose abuse, sexual requests or other misuses against them to a member of staff, they can use the Report Abuse button ([www.thinkuknow.co.uk](http://www.thinkuknow.co.uk))[[1]](#footnote-1) to make a report and seek further advice. The issue of a pupil deliberately misusing online technologies should also be addressed by the establishment.

Pupils should be taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, as this may have legal implications.

# **Associated Policies**

Keeping Records and Data Protection

IT, internet and online safety

Mobile Phone Policy

Behaviour Policy

Safeguarding Policy

Disciplinary Policy

Incident and Serious Incident Requiring Investigation Policy

Whistle Blowing

# **Useful Links – E Safety information and support**

[www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/](http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/)

[www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

[www.disrespectnobody.co.uk](http://www.disrespectnobody.co.uk)

[www.saferinternet.org.uk](http://www.saferinternet.org.uk)

[www.internetmatters.org](http://www.internetmatters.org)

[www.pshe-association.org.uk](http://www.pshe-association.org.uk)

[www.educateagainsthate.com](http://www.educateagainsthate.com)

[www.ceop.police.uk/](http://www.ceop.police.uk/)

[www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation](http://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation)

**Screening and confiscation**

<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

**Manchester Safeguarding Partnership**

[Page not found : Manchester Safeguarding Boards (manchestersafeguardingpartnership.co.uk)](https://www.manchestersafeguardingpartnership.co.uk/policies-resources/)

**Related Legislation**

We are aware of the legislative framework under which this E-Safety Policy and guidance has been written. It is important to note that in general terms, an action that is illegal if committed offline, is also illegal if committed online. Where appropriate and when recommended, the school will ensure legal advice is sought in the event of an e-safety issue or situation.

Keeping Children Safe in Education 20122

Criminal Justice and Courts Act 2015

Criminal Justice & Public Order Act 1994

Sexual Offences Act 2003

Computer Misuse Act 1990

Data Protection Act 1998 and 2018

Freedom of Information Act 2000

Communications Act 2003

Malicious Communications Act 1988

Regulation of Investigatory Powers Act 2000

Racial and Religious Hatred Act 2006

Protection from Harassment Act 1997

Public Order Act 1986

Obscene Publications Act 1959 and 1964

Human Rights Act 1998

The Education and Inspections Act 2011

**Searching, Screening and Confiscation;**

<https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/444053/Searching_screening_confiscation_advice_Reviewed_July_2015.pdf>

The Protection of Freedoms Act 2012

 ****

**Appendix 1 – ICT User Agreement – Years 1 – 3**

Our ‘Think then Click’ rules will help us to stay safe on the internet in school and at home.

 We tell an adult if someone we don’t know asks for personal information on the internet.

 We tell an adult if we receive a message which is not nice.

 We ask permission before using the internet.

 We only use websites that an adult says are OK.

 We tell an adult if we see anything we are uncomfortable with.

 We immediately close any webpage we are not sure about.

 We only message people an adult has said it’s ok to.

 We send messages that are polite and friendly.

 We never give out personal information or passwords.

 We never arrange to meet anyone.

 We do not use internet chatrooms.

 We do not download anything without checking that it is ok first.

Pupil name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pupil signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 

**Appendix 2 – ICT User Agreement – Years 4 – 6**

Our ‘Think then Click’ rules will help us to stay safe on the internet in school and at home.

 I will only use ICT in school for school purposes.

 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 look for, 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 from the internet.

I will not send my image unless this is part of a school project and approved by my teacher.

I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.

I will support the school approach to online safety and not 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 not sign up for any online service unless this is an agreed part of a school project approved by my teacher.

I will not sign up to online services until I am old enough.

I understand that the school may take action if I do not follow the above rules in school and out of school. This may include my parents/carers being contacted.

Pupil name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Pupil signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 3 – ICT Parent User Agreement**

As the parent/carer of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ I give permission for my child to have access to the internet and to ICT systems at school. I know that my child has signed an Acceptable Use Agreement and has received/will receive E-safety education. This will help them to understand that the school the importance of safe use of ICT in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when using the internet and ICT systems. I also understand that the school cannot be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my child’s activity on ICT systems will be monitored and that school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home. I will ensure that my child is supervised whilst on the internet and I will monitor their online activity. I will inform the school if I have any concerns over my child’s E-safety.

Parent/carer name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Parent/carer signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Appendix 4 – ICT User Agreement – Community**

This Community User Acceptable Use Agreement is to assist visitors to Unity Community Primary School, in staying safe and to protect the security and integrity of the school’s ICT systems.

* I understand that any personal equipment brought into school remains my sole responsibility.
* I will only use the school’s ICT for professional purposes.
* I will comply with the ICT system security and not disclose any passwords required by any of the programmes or systems that I use. If I have any reason to believe that a password has been compromised I will immediately ask for a new one to be issued.
* I understand that I am responsible for all activity carried out on the school’s ICT systems, or via the school’s internet connection, and that my usage will be monitored and logged.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
* I will not install any hardware or software without the permission of the Headteacher.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of students and/or staff will only be taken, stored and used for professional purposes in line with school policy.
* I will respect copyright and intellectual property rights.
* I will report any incidents or concern regarding children’s safety to the Headteacher or other Designated Safeguarding Lead.
* I will report any damage to, or malfunction of, any ICT equipment to the school.

Community user name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Community user signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. [↑](#footnote-ref-1)