

Ranvilles Junior School  
Computing,  
Information Communication Technology and  
Online Safety Policy

**1. ACCESSIBILITY**

This policy is available in large print or Braille. Please contact the school office who will be happy to arrange this for you.

**2. PURPOSE OF POLICY**

This policy outlines the schools policy on:

- Teaching and Learning of Computing
- Information Communication Technology (ICT) – Equipment and Usage
- Online Safety

The guidelines are drawn up to ensure all stakeholders within the school are aware of what is expected of them and are able to stay safe when using the hardware and software we have in school. The equipment and resources within the school are provided to enhance the learning of the pupils and to aid the staff in their delivery of the curriculum; this policy will enable these to go ahead.

**3. APPROVAL**

Approval date: February 2024

Approver: Amanda Stevens

Approver position: Chair of Governors

Date for next review: February 2026

#### **4. INTRODUCTION**

This policy will set out a framework for:

- 1) how Computing is taught, monitored and assessed throughout the school
- 2) how ICT is used as a tool for teaching and learning as well as communication
- 3) how we teach and manage Online Safety

This policy has been written with guidance and support from other teachers, schools and local authorities and aims to meet the criteria established by organisations such as DfE, Naace and 360safe. The school uses the 360safe online self-review tool to measure its effectiveness and action plan for improvement. Other schools will have a number of policies including Online Safety and Social Media, but as a school Ranvilles Junior has decided to combine them into one policy.

#### **5. REFERENCES**

- 360safe
- Naace
- DfE Teaching Online Safety in School – June 2019
- Education for the Connected World – 2020 edition
- Teacher Standards 2011 (terminology updated Dec 2021)

#### **6. TEACHING AND LEARNING**

##### **6.1 The Curriculum**

The Computing Curriculum is made up of 3 strands:

- Computer Science – programming, networking
- Information Technology – software skills, hardware skills, generic skills
- Digital Literacy – Online safety, digital citizen

Computing is taught across the curriculum and wherever possible, integrated into other subjects. Pupils receive a once weekly lesson focused on computing skills which can then be applied in the cross-curricular classroom. Digital Literacy is taught and applied through computing lessons. In addition, every year group completes comprehensive units of work on an aspect of Online Safety in PSHE – see PSHE Long Term Map. Pupils may be taught computing using desktop computers, laptops or tablets. The long term computing map shows the journey that the pupils are expected to take but this is adapted to ensure it is relevant and up to date. Agreed Procedures are in place which outline how computing is taught in school.

The Computing Leader ensures that the plans provide coverage of what is expected.  
The Computing Leader ensures that the pupils are challenged and are able to succeed.

##### **6.2 – How ICT is used to support Teaching and Learning**

ICT encompasses every part of modern life and it is important that our pupils are taught how to use these tools and more importantly, how to use them safely. We believe it is important for pupils, staff and the wider school community to have the confidence and ability to use these tools to prepare them for an ever-changing and rapidly developing world. To enable all our staff and pupils to be confident, competent, independent users and learners of ICT we aim to:

1. Use ICT where appropriate to ensure pupils are motivated and inspired in all areas of the curriculum
2. Use ICT to help improve standards in all subjects across the curriculum
3. Develop the ICT competence and skills of pupils through ICT lessons and provide them with the chance to consolidate these in a cross-curricular context
4. Ensure pupils are challenged in their use of ICT and are provided with exciting, creative ways in which to share their learning
5. Use tools available to ensure pupils have the ability to work independently and collaboratively to suit the needs of the situation
6. Provide all staff with the training and support to ensure that they can, and have the confidence to, use ICT to its full potential in all aspects of school life
7. Use ICT as a form of communication with parents, pupils and the wider community

#### **6.4 Online/Remote Learning**

As more of the world moves online, we recognise the need to provide pupils with opportunities to be confident users of online resources. Teachers guide pupils to a range of online resources that are deemed age appropriate to support their current learning.

On entry to the school, pupils/parents are provided with online access to:

- a) Our online platform designed as a communication tool with the whole school and individual parents and learners
- b) Our Virtual Classroom for online learning – using G Suite for Education
- c) A number of online platforms to support reading, spelling and maths
- d) A school email address linked to our virtual classroom

All of the platforms used are accessible only to pupils, staff and parents of our school community.

Guidance on how to access and use these resources is shared with parents and pupils and they are taught how to use them safely.

Homework is set and submitted online through our virtual classroom. This classroom is also in place for the event of a school closure.

The school is mindful of pupils who may not have the appropriate access to technology at home and focuses to support these families.

#### **6.5 G Suite for Education**

The school's online learning space is set up through G Suite for Education. This is a free system which includes many of the products, including Gmail, Calendar, Docs, Forms, Slides, Meet, and more. The pupils will be gradually be given permission to use the different tools according to their age and online safety awareness. Pupils may need to prove they can use the tools safely before having them enabled. Schools own their own data on G Suite for Education; Google keep it safe using secure servers and platform services.

Every staff member and child is provided with a new Google Account for G Suite for Education. They should not use existing, personal accounts. This enables the school to use the appropriate online privacy & security settings, protecting pupils' data in their school account from being stored, repurposed, or provisioned by third parties, especially when it comes to personal information.

## **6.6 Assessment**

Computing is assessed in a number of ways using formative and summative assessment. Formative assessment happens during computing lessons and is used to inform future planning; this is conducted by a teacher on an informal basis. Summative assessments are made at the end of a unit of work against core skills that have been directly correlated to the National Curriculum. Age related developmental skills are tracked and used to inform teaching and learning as well as to report to parents.

## **6.7 Equal Opportunities and Inclusion**

The school ensures that all pupils are provided with opportunities to access the Computing curriculum throughout the school. Where necessary, staff endeavour to make adaptations to the environment or provide software that enables all learners to achieve. The school's SENDCo identifies specific IT based programmes and hardware for pupils who require this additional support. The Deputy Headteacher monitors IT access at home.

## **7. INFORMATION COMMUNICATION TECHNOLOGY – EQUIPMENT AND USE**

The world of ICT is forever changing and developing and as such Ranvilles endeavours to ensure pupils have access to high quality teaching and resources to ensure they are competent, confident and independent users. In school pupils have access to a range of equipment including desktop computers, laptops, tablets, cameras, digital microscopes, data loggers to name but a few. Pupils are taught how to use this equipment effectively and safely.

### **7.1 Technical – infrastructure/equipment, filtering and monitoring**

The school ensures that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Through monitoring, the school ensures that the relevant people named in the above sections are effective in carrying out their online safety responsibilities:

- School technical systems are managed in ways that ensure that the school meets recommended technical requirements
- There are regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling are securely located and physical access restricted
- The IT Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users by Agile. Illegal content (e.g. abusive child images) is filtered by the filtering provider. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- Internet filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet
- The school has provided enhanced/differentiated user-level filtering – this allows different filtering levels for pupils and staff
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software

### **7.1.1 User Access**

- All users have clearly defined access rights to school technical systems and devices.
- All users are provided with a username and secure password by the IT Manager who keeps an up to date record of users and their usernames. Users are responsible for the security of their username and password. Staff should not share their details with any other member of staff or child.
- It is the responsibility of the office staff to inform the IT Manager of the child's name and class. The IT Manager will then provide a network log in. The Admin Officer creates accounts for the online applications used by the school.
- Once pupils have left the school, the child's account is removed from their online applications and their content is removed. They are also removed from the school system.
- The "master/administrator" passwords for the school systems, used by the IT Manager / Admin Officer are also available to the Headteacher or other nominated senior leaders and kept in a secure place.
- Trainee teachers are provided with temporary access to the school systems for the duration of their time at Ranvilles. They will be required to adhere to and sign the staff user agreement.
- Supply teachers are provided with temporary access to the school system where only access to the learning resources and key information they require is accessible for the duration of their time at Ranvilles. They will be required to adhere to the staff user agreement whilst at the school.
- Staff must seek permission before installing hardware or downloading software onto the school computer from the Headteacher and/or computing leader.
- Teachers are provided with a school laptop for work. They sign a Loan Agreement and also an Acceptable Use Agreement. These should all be password protected. Staff should be vigilant to not leave their laptop or device lying around or on display. Personal data should not be transferred onto devices.
- Staff should avoid the use of memory sticks and no staff or pupil data should be saved on a memory stick – this is all accessible through Remote Access or online on Insight.
- In the event of a school closure, hardware may be loaned to parents of pupils who do not have equipment at home to support their learning. They sign a Loan Agreement to take responsibility for the equipment.
- Pupils should not bring memory sticks into school. If they wish to share work in school that they have completed on the computer, they may email it to the school office for the attention of the teacher, or submit it through one of the two virtual platforms.
- All pupils sign and parents counter-sign an Acceptable Use Agreement at the start of every academic year. Pupils are issued with a username and password on joining the school.

### **7.1.2 Mobile Technologies**

The primary purpose of the use of mobile devices in the school is educational.

Staff mobile phones should not be on view or used in the classroom. Some pupils may bring their mobile phone into school (although this should only be if they are walking to and from school on their own) and these should be handed into the school office for safe storage throughout the day. Pupils should not use their phones on school site.

No videoing or photographing should take place on a personal mobile phone – staff or pupils.

The school acceptable use agreements for staff, pupils/students and parents/carers give consideration to the use of mobile technologies

## **7.2 Network / School Server**

The school server is run by Agile. It is backed up remotely. The school IT Manager runs basic housekeeping on the server.

## **7.3 Internet and E-mail**

The internet may be accessed by staff and by pupils throughout their hours in school.

The teaching of email and internet use is covered with the computing curriculum planning, but staff should encourage regular dialogue that explores the benefits and potential dangers of using the internet.

All members of staff are issued with a school email address and this is the email which they should use for professional communication. Staff should take extra care to ensure that all communication with pupils and/or parents remains professional. Users are responsible for all messages that are sent and due regard should be paid to the content of emails to ensure it is not misconstrued. All web activity is monitored by the IT Manager. It is the user's responsibility to ensure they log off or lock their computer appropriately.

Pupils have a G Suite for Education email address linked to the Virtual Classroom.

## **7.4 Passwords**

Staff should make sure that any passwords they use are strong and contain a mixture of the following: upper- and lower-case letters, numbers and punctuation. Passwords should be long and memorable for the user but not something that would be familiar to other people.

The IT Manager enforces a password change every 3 months. However, staff members should change their password if they suspect others may know it. Passwords should never be shared. They should ideally be different for each application to support the security of these tools.

Pupils are taught about the importance of passwords and their protection. They are issued with individual passwords for all the applications they are given access to at school. They should keep these confidential too. The IT Manager, computing lead and class teacher have access to these passwords should pupils forget them. Pupils' school computer accounts are also password protected.

## **7.5 External Communication**

### **7.5.1 School Website**

The school website is overseen by the Headteacher, Computing Leader and Website Coordinators. It is updated to be reflective of current practice in school. It is used to share information about the school with people inside and outside our school community.

### **7.5.2 Email and Text Messaging**

School communications with parents may be sent via email or text message using the Arbor system. Hard copies of information are only sent home if requested by a parent/guardian.

### **7.5.3 Virtual Platform**

Ranvilles Virtual Platform is the form of communication between school and home. Letters are posted on the School Story page and Arbor via an email. Individual messages can be sent from Arbor and other members of the school community on here too. Pupils cannot message teachers directly through their accounts.

### **7.5.4 Facebook / Twitter**

The school has a Facebook page and Twitter account. These are managed by one of the Website Coordinators. The purpose is to share information about the school to the wider community.

## **8. ONLINE SAFETY**

The National Curriculum 2014 states:

*Pupils should be taught to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*

The internet is an essential element in 21<sup>st</sup> century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Pupils use the internet widely outside school and will need to learn how to evaluate internet information and to take care of their own safety and security.

### **8.1 Scope of the Policy**

The Education and Inspections Act 2006 empowers Headteachers to such an extent as is reasonable, to regulate the behaviour of pupils when they are off school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside 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. The school deals with such incidents within this policy and associated behaviour and anti-bullying policies and, where known, informs parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

### **8.2 Roles and Responsibilities**

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

#### **8.2.1 Governors**

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This is carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs



- reporting to relevant Governors meeting

### **8.2.2 Headteacher and Senior Leaders**

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the Online Safety Lead.

The Headteacher and Senior Leadership Team:

- know the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- regularly receive monitoring reports from the Online Safety Lead

### **8.2.3 Online Safety Lead**

The Online Safety Lead (typically the Computing Leader):

- leads the Online Safety Group
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Senior Leadership Team

### **8.2.4 IT Manager**

Those with technical responsibilities are responsible for ensuring:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; Online Safety Lead for investigation/action/sanction



- that monitoring software/systems are implemented and updated as agreed in school policies

### **8.2.5 Teaching and Support Staff**

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use agreement (AUA)
- they report any suspected misuse or problem to the Headteacher/Deputy Headteacher /Online Safety Lead) for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- 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

### **8.2.6 Designated Safeguarding Lead and CPLOs**

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

### **8.2.7 Online Safety Group**

The Online Safety Group provides a consultative group that has wide representation from the school community – a senior leader, a teacher, a teaching assistant, IT Manager, a parent, pupils and Online Safety Governor - with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group will assist the Online Safety Lead with:

- the production/review/monitoring of the school online safety policy/documents
- the production/review/monitoring of the school filtering and requests for filtering changes
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

### **8.2.8 Pupils:**

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

### **8.2.9 Parents/carers**

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school takes every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents and carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line pupil records
- their children's personal devices in the school

### **8.2.10 Community Users**

Community Users who access school systems or programmes as part of the wider school provision are expected to sign a Community User AUA before being provided with access to school systems.

## **8.3 Education and Training**

### **8.3.1 Education – Pupils**

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety is a focus in all areas of the curriculum and staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and is provided in the following ways:

- A planned online safety curriculum provided as part of the Computing and PHSE curriculum. Online safety messages are regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies
- Pupils are taught, in all lessons, to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons, where internet use is pre-planned, it is best practice that pupils are 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.
- Where pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

### **8.3.2 Education – Parents/carers**

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site, Learning Platform
- Parents/carers sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

### **8.3.3 Education & Training – Staff/Volunteers**

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training is offered as follows:

- A planned programme of formal online safety training (Educare) is made available to staff. This is regularly updated and reinforced. An audit of the online safety training needs of all staff is carried out regularly.
- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) receives regular updates through attendance at external training events (e.g. from SWGfL/LA/other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates are presented to and discussed by staff in staff/team meetings/training sessions.

- The Online Safety Lead (or other nominated person) provides advice/guidance/training to individuals as required

### **8.3.4 Training – Governors/Directors**

Governors/Directors take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisations (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

### **8.3.5 Use of digital and video images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils 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 online-bullying 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 informs and educate users about these risks and implement policies to reduce the likelihood of the potential for harm. The school adopts the following practice:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website/social media/local press.
- 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 are selected carefully and comply with good practice guidance on the use of such images.
- Pupils' full names are not be used anywhere on a website or blog, particularly in association with photographs.

### **8.3.6 Data Protection**

See the schools' Data Protection policy.

## **8.4 Communications**

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies, the school considers the following as good practice:

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information must not be posted on the school website and only official email addresses should be used to identify members of staff.

## **8.5 Social Media - Protecting Professional Identity**

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm are in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Providing training including: acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference is made in social media to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions are not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
  - Systems for reporting and dealing with abuse and misuse

- Understanding of how incidents may be dealt with under school disciplinary procedures

#### **8.5.1 Personal Use:**

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

#### **8.5.2 Monitoring of Public Social Media:**

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school effectively responds to social media comments made by others according to a defined policy or process

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

### **8.6 Dealing with unsuitable/inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and is obviously banned from school and all other technical systems. Other activities e.g. cyber-bullying are banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school has identified the activities they believe to be inappropriate in a school context and that users should not engage in these activities in/or outside the school when using school equipment or systems.

### **8.7 Responding incidents of misuse**

#### **8.7.1 By staff**

Failure to comply with the guidelines and expectations set out for them could lead to sanctions being imposed on staff and possible disciplinary action being taken in accordance with the school's policy and possibly law.

#### **8.7.2 By pupils**

Pupils should be aware that all online safety issues will be dealt with quickly and effectively. When dealing with unacceptable use, staff should follow the behaviour policy and if necessary, the anti-bullying policy. Pupils may have restrictions placed on their account for a short time.



## 8.8 Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the **Flowchart for Responding to Inappropriate or Illegal Incidents** (Appendix 1) for responding to online safety incidents and report immediately to the police.

## 8.9 Other Incidents

It is hoped that all members of the school community are responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. See appendices for how to deal with these issues.

## 8.10 School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures and the actions and outcomes are reported to the Computing Leader and Senior Leadership Team.

## 9. APPENDICES

### APPENDIX 1 - DEALING WITH MISUSE

**In the event of suspicion, all steps in this procedure should be followed:**

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national/local organisation (as relevant).
  - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
  - incidents of ‘grooming’ behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material

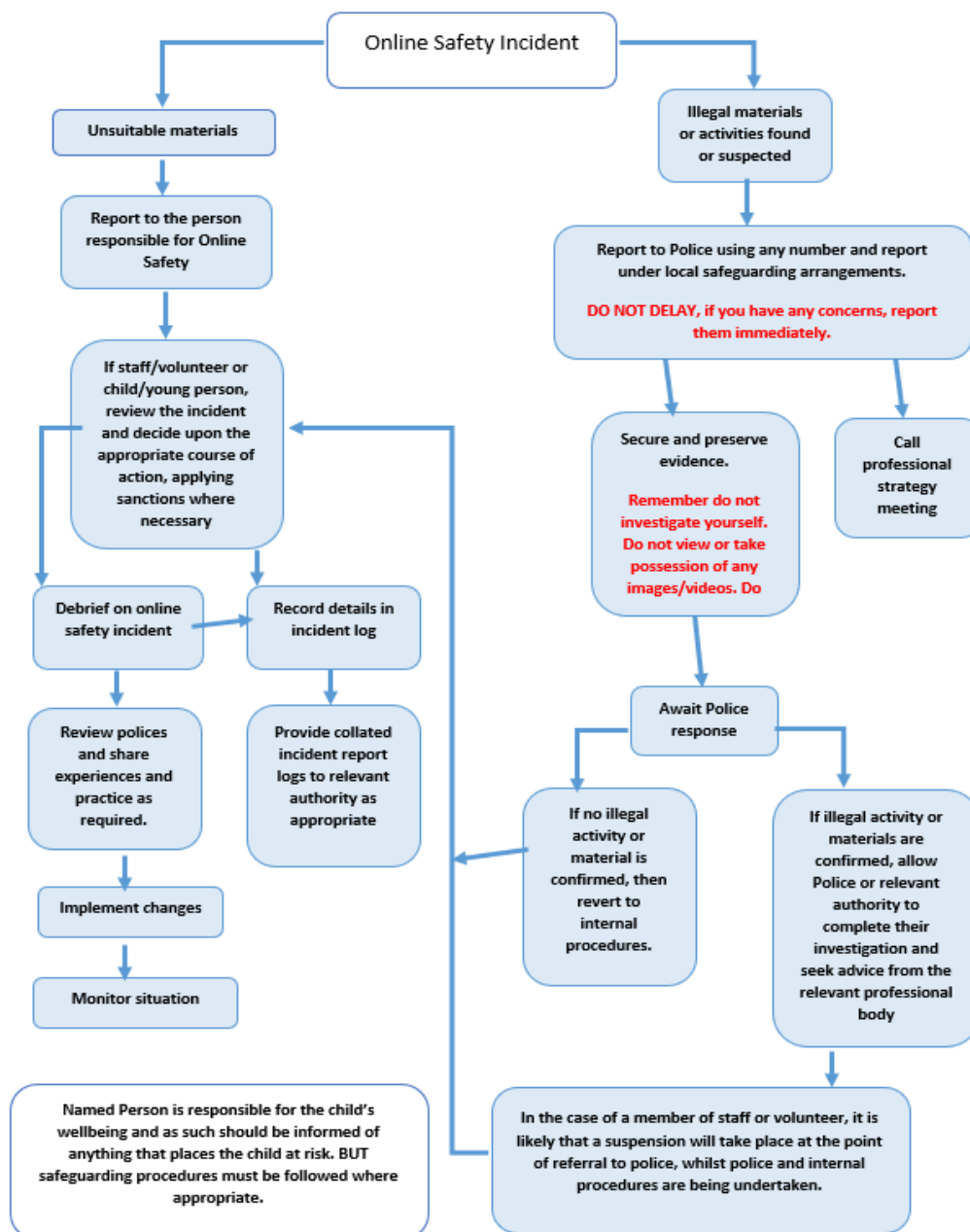
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

### Flowchart for Responding to Inappropriate or Illegal Incidents

Any concerns of inappropriate or illegal incidents must be reported to the Headteacher in line with the safeguarding policy. Below is the flowchart that the Headteacher will follow when dealing with online incidents.



## APPENDIX 2 Unsuitable / Inappropriate Activities

Some internet activity is illegal and this is obviously banned from school and all other technical systems. Other activities are banned and could lead to criminal prosecution. There are also a number of activities, which are considered legal, but would be deemed inappropriate due to the age of users or nature of activities.

Below is a list of activities deemed inappropriate and unacceptable at Ranvilles Junior School. The school believes that the activities referred to would be inappropriate in school context and that users should not engage in these activities in or out of school when using school equipment or systems.

User Actions		Unacceptable and Illegal	Unacceptable	Acceptable for nominated users	Acceptable at certain times	Acceptable
Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.  <a href="#">Refer to RJS Safeguarding Policy regards dealing with self-generated images/sexting.</a>	x				
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003	x				
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008	x				
	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	x				
	Pornography		x			
	Promotion of any kind of discrimination		x			
	Threatening behaviour, including promotion of physical violence or mental harm		x			
	Promotion of extremism or terrorism		x			
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute		x			
Activities that might be classed as cyber-crime under the Computer Misuse Act: <ul style="list-style-type: none"> <li>Gaining unauthorised access to school networks, data and files, through the use of computers/devices</li> <li>Creating or propagating computer viruses or other harmful files</li> <li>Revealing or publicising confidential or proprietary information (e.g. financial, personal information,</li> </ul>	x					

databases, computer / network access codes and passwords					
<ul style="list-style-type: none"> <li>• Disable/ impair/disrupt network functionality through the use of computers/devices</li> <li>• Using penetration testing equipment (without relevant permission)</li> </ul>					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school		x			
Revealing or publicising confidential or propriety information (e.g. financial/personal information, databases, computer/network access codes and passwords)		x			
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)		x			
Using school systems to run a private business		x			
Infringing copyright		x			
On-line gaming (educational)					x
On-line gaming (non-educational)		x			
On-line gambling		x			
On-line shopping/commerce			x		
File sharing				x	
Use of social media			x		
Use of messaging apps (school approved – ClassDojo, Arbor)					x
Use of video broadcasting e.g. YouTube (teachers only)			x		

### APPENDIX 3

## Ranvilles Junior School Staff and Volunteer ICT Acceptable Use Agreement

### School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

### This acceptable use policy is intended to ensure:

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff are protected from potential risk in their use of technology in their everyday work

The school will try to ensure that staff and volunteers have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

## Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

Professional and personal safety:	<ul style="list-style-type: none"> <li>• I understand that the school will monitor my use of the school digital technology and communications systems.</li> <li>• I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.</li> <li>• I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.</li> <li>• I will not disclose my usernames or passwords to the school system and applications to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.</li> <li>• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.</li> </ul>
Professional communication and action on school system:	<ul style="list-style-type: none"> <li>• I will not access, copy, remove or otherwise alter any other user's files, without their express permission.</li> <li>• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.</li> <li>• I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless given permission to do so by the Headteacher. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.</li> <li>• I will only use social networking sites in school in accordance with the school's policies.</li> <li>• I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.</li> <li>• I will not engage in any on-line activity that may compromise my professional responsibilities.</li> </ul>
Safe and secure access to technologies:	<ul style="list-style-type: none"> <li>• When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.</li> <li>• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)</li> <li>• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security</li> </ul>

	<p>systems in place to prevent access to such materials.</p> <ul style="list-style-type: none"> <li>• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.</li> <li>• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, without the permission of the Headteacher.</li> <li>• I will not disable or cause any damage to school equipment, or the equipment belonging to others.</li> <li>• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Personal data should not be taken out of the school system – remote access is available for use outside of the school building. Paper based documents containing personal data must be held in lockable storage.</li> <li>• I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.</li> <li>• I will immediately report any damage or faults involving equipment or software, however this may have happened.</li> </ul>
Everyday use:	<ul style="list-style-type: none"> <li>• I will use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines.</li> <li>• I will log off when I have finished using a computer.</li> <li>• I will make use of digital technologies in school and ensure they are returned after use ensuring pictures/files are removed ready for the next person's use.</li> <li>• I will try not to be wasteful with equipment – paper, ink etc.</li> <li>• I will report any issues to the SLT or IT leader as soon as possible.</li> <li>• I will return any hardware or equipment when I am no longer employed by the school.</li> </ul>
Using the internet in professional capacity:	<ul style="list-style-type: none"> <li>• I will ensure that I have permission to use the original work of others in my own work.</li> <li>• Where work is protected by copyright, I will not download or distribute copies (including music and videos).</li> </ul>
Responsible Use:	<ul style="list-style-type: none"> <li>• I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.</li> <li>• I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.</li> </ul>

**Declaration:**

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer	Signed	Date



## APPENDIX 4

### Ranvilles Junior School Pupil ICT Acceptable Use Agreement

Digital technologies have become an important part of our lives, both in and out of school. The internet and other communication technologies are powerful tools, which open up new opportunities for everyone. These technologies are great for learning as they can stimulate discussion and collaboration, promote creativity and can help us find information quickly.

#### This agreement is intended to make sure that:



- you know how to be responsible users of the Internet and other communications technologies at home and at school
- you know how to keep yourself, others, our school and your home safe






The school will try to ensure that you have good access to ICT to enhance your learning and will, in return, expect you to agree to be responsible users.

#### Acceptable Use Agreement

- I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users

The following actions will help to keep you, other people, our school and your home safe. They are relevant to home and school and whenever and wherever you are using the Internet or communication device, for example computers, laptops, tablets, games consoles, phones etc.

<p>For my own personal safety...</p> 	<ul style="list-style-type: none"> <li>• I understand that the school will monitor my use of the systems, devices and digital communications.</li> <li>• I will keep my usernames and passwords for school systems and applications safe and secure – I will not share them, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.</li> <li>• I will be aware of "stranger danger", when I am communicating on-line.</li> <li>• I will not share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, photographs, videos, educational details etc.)</li> <li>• I will not arrange to meet people off-line that I have communicated with on-line without permission from my parent or carer. If they give permission, I will always meet in a public place and take my parent or carer with me.</li> <li>• I am aware that the Internet contains information that is: inaccurate, harmful, illegal, commercial and inappropriate.</li> <li>• I will immediately report to an adult anything unpleasant or that I know is inappropriate or makes me feel uncomfortable.</li> </ul>
<p>Equal rights to use technology as a resource...</p> 	<ul style="list-style-type: none"> <li>• I understand that the purpose of ICT in school is to support my learning and that's what I will use it for.</li> <li>• I will use computers and devices when I have permission. In school, I must be supervised and at home, will follow any family agreement about using computers and devices.</li> <li>• I will seek permission from my teacher before I download or upload work.</li> <li>• I will only use the school systems or devices for educational on-line games and learning opportunities. I will always ask permission to use the systems for other activities.</li> <li>• I will use the computer/devices that are allocated to me and will take care of the additional equipment assigned to that device.</li> </ul>

<p>Respecting others...</p> 	<ul style="list-style-type: none"> <li>• I will respect others' work and will not open, copy, remove or otherwise change any other people's files or folders without permission.</li> <li>• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I understand that others may have different opinions.</li> <li>• I will make sure people are happy before I take a photograph of them. I will not share images of anyone without their permission.</li> <li>• I will only use the photos I have taken with adult permission and will not name people in my photos.</li> </ul>
<p>Looking after equipment at school and at home...</p> 	<ul style="list-style-type: none"> <li>• I understand that I cannot use my mobile phone in school and must turn it off when arriving at school and hand it in to my teacher for safekeeping.</li> <li>• I will not install any software or hardware without permission from my teacher. If I wish to share something from home, I may email it to school or upload it to the school's virtual learning platform.</li> <li>• I will immediately report any damage or faults involving equipment or software, however this may have happened.</li> <li>• I will prevent viruses spreading by only opening emails and attachments from people I trust.</li> <li>• I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.</li> <li>• I will follow the school's procedures for saving work, naming documents appropriately and saving regularly to protect my work.</li> </ul>
<p>When using the internet for research or recreation...</p>  	<ul style="list-style-type: none"> <li>• I will use known websites that my parents/teachers know about and are happy with.</li> <li>• I will use children's search engines when looking for information or images.</li> <li>• I will respect other people's work on the Internet and not copy it without saying where it came from.</li> <li>• Where work is protected by copyright, I will not try to download copies (including music and videos)</li> <li>• When I am using the internet to find information, I will take care to check that the information that I access is accurate.</li> <li>• Social media sites have age restrictions in place and I will not access or use sites that are inappropriate for my age. I understand that I am not allowed to access social media in school.</li> </ul>
<p>Being a responsible user...</p> 	<ul style="list-style-type: none"> <li>• I understand that if I am acting inappropriately and choose not to follow this agreement, in school or out of school, where my actions involve my membership of the school community (examples would be online-bullying, use of images or personal information), that the school will implement appropriate consequences. This may include loss of access to the school network/internet/devices, loss of free time, exclusions, and contact with parents and in the event of illegal activities involvement of the police.</li> </ul>

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

## Pupil ICT Acceptable Use Agreement Form



I have read and understand the Acceptable Use Agreement and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed)
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website, virtual learning platforms etc.

Name of Pupil	Class	Signed	Date

### Parent Declaration

I have read this agreement with my child and reinforced the importance of online safety and acceptable use at school and at home. I agree with the contents and will support the school in its implementation.

Parent/Guardian	Signed	Date

Please tick one of the following:

I am aware of the dangers of using ICT technologies and the Internet and understand how to take precautions to protect my child at home, for example using children logins, filtering and monitoring, supervised use and family agreements for use.

I would be interested in attending an eSafety meeting to find out more about the dangers of ICT technologies and the Internet and how to take precautions to protect my child at home.

## APPENDIX 5

### Ranvilles Junior School Community ICT Acceptable Use Agreement

**This acceptable use agreement is intended to ensure:**

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that users are protected from potential harm in their use of these systems and devices

#### Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person
- I will not access, copy, remove or otherwise alter any other user's files, without permission
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos)
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

## Collecting Personal Data

Please see the table below which identifies how your data will be stored.

<b>Who will have access to this form?</b>	Members of Senior Leadership Team and IT leader and Manager.
<b>Where will this form be stored?</b>	In a locked storage unit.
<b>How long will this form be stored for?</b>	The form will be stored for the duration of time the Community User is accessing the school's systems.
<b>How this form will be destroyed?</b>	The form will be shredded when the user is no longer accessing school systems.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

<b>Community User</b>	<b>Company</b>	<b>Signed</b>	<b>Date</b>