Rye Community Primary School Policy

Policy Title:	eSafety
Leadership Responsibility:	Designated Safeguarding Lead
Review Body:	Executive Headteacher
Date:	December 2021
Review:	December 2022

Context

Our academy recognises the importance of treating eSafety as an ever-present serious safeguarding issue. It is important to protect and educate both pupils and colleagues with supportive mechanisms, policies and protocols to protect and support the community.

Ofsted reviews eSafety measures in academies and there are numerous Acts of Parliament which can be used to safeguard both pupils and colleagues in academies. The safeguarding aspects of eSafety are evident in all our ICT and safeguarding policies and procedures throughout the academy, and it is essential that this constantly developing area of technology is kept under review.

This policy links all the ICT, safeguarding and other policies and procedures to reflect how the academy deals with eSafety issues daily. This policy should also be read in conjunction with the home learning policy. The documents referred to in this eSafety policy have been developed by various groups including:

- Advisory Council Members in other Academies;
- Headteachers, Leaders, Designated Safeguarding Leads;
- ICT Subject Leaders and IT technical support;
- Teachers and associate colleagues;
- Parents and families;
- Pupils.

Objectives and targets

This policy is aimed at making the use of electronic communication at Rye Community Primary School as safe as possible. This policy applies to all members of the academy community (including colleagues, pupils, volunteers, parents, families, visitors, community users) who have access to, and are users of, academy ICT systems, both in and out of academy.

Action plan

The academy will deal with any eSafety incidents which arise by invoking this policy, other ICT policies and the associated behaviour and anti-bullying policies. The academy will, where known, inform parents of incidents of inappropriate eSafety behaviour that take place out of academy and take appropriate action.

The following sections outline:

- The roles and responsibilities for eSafety of individuals and groups within the academy, and how they will receive education/training to fulfil those roles;
- How the infrastructure is managed;
- How eSafety is considered in the curriculum;
- The protocols on using digital images;
- The protocols on data protection;
- The protocols for handling electronic communication;
- Awareness of and dealing with inappropriate use of electronic media.

Roles and responsibilities – Executive Headteacher

- The Executive Headteacher is responsible for the eSafety policy and for reviewing the effectiveness of the policy.

Roles and responsibilities – Advisory Council

- Mrs Nice is the nominated link for eSafety and an appointed member of the academy's eSafety committee.
- The Advisory Council receives eSafety training/awareness sessions as part of their regular cycle of meetings.

Roles and responsibilities – Head of School and senior leaders

- The head of school is responsible for ensuring the eSafety of members of the academy community;
- The head of school and other members of the leadership team will be aware of the procedures to be followed in the event of a serious eSafety allegation being made against a member of staff, including the head teacher;
- The Education and Inspections Act 2006 empowers the head teacher, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other eSafety incidents covered by this policy, even though they may take place out of academy, but are linked to membership of the academy.

Roles and responsibilities – eSafety co-ordinator

- There is a collaborative approach to eSafety at Rye Primary and Mrs Nice works alongside the members of the relevant curriculum working party to achieve this. However, Mrs Nice is the designated e safety coordinator and as such;
- Takes day-to-day responsibility for eSafety issues and has a leading role in establishing and reviewing the academy eSafety policy and other related policies;
- Ensures that all members of staff are aware of the procedures that need to be followed in the event of an eSafety incident taking place;
- Provides training and advice for staff;
- Liaises with the trust and local authority as necessary;
- Liaises with academy IT technical staff;
- Reports regularly to the leadership team and head teacher.

The eSafety co-ordinator (or other nominated person) will receive training at regular update sessions and by reviewing national and local guidance documents.

Roles and responsibilities – network manager/technical support provider

The network manager or technical support provider is responsible for ensuring:

- That the academy's ICT infrastructure is secure and is not open to misuse or malicious attack;
- That the academy meets the eSafety technical requirements outlined in the relevant national/local ICT security policy and/or acceptable usage/eSafety policy and guidance;
- Users may only access the academy's networks through a properly enforced password protection policy.

Roles and responsibilities – teaching and support staff

Teaching and associate colleagues are responsible for ensuring that:

- They have an up-to-date awareness of eSafety matters and of the current academy eSafety policy;
- They have read, understood and signed the relevant staff acceptable computer usage agreement and staff laptop usage agreement, as well as other related policies e.g. staff email, social media policies;
- They report any suspected misuse or problem to the head teacher, Business manager or IT Network Manager as appropriate for investigation;
- Digital communications within the academy (email/virtual learning environment (VLE)/voice) should be on a professional level and only carried out using official academy systems;
- Pupils understand and follow the academy eSafety policy and the pupil acceptable computer usage policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- They monitor ICT activity in lessons, extracurricular and extended academy activities;
- They are aware of eSafety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current academy policies regarding these devices;
- They are aware of the eSafety issues pertaining to email and social media usage;
- 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.

All staff members receive eSafety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal eSafety training will be made available to staff. An audit of the eSafety training needs of all staff will be carried out regularly;
- All new staff will receive eSafety training as part of their induction programme, ensuring that they fully understand the academy eSafety policy and acceptable usage policies.

Roles and responsibilities – designated person for child protection/child protection officer

The designated person for child protection/child protection officer is trained in eSafety issues and will be aware of the potential for serious child protection 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;
- Cyber-bullying.

Roles and responsibilities – eSafety group

Members of the eSafety group (link AAC member, SLT member, staff member, pupil member, parent representative, and network manager) will assist with the development of eSafety education.

At Rye Community Primary School, we feel that it is important that our children have a robust understanding of e-safety education. We seek to develop their understanding through a whole school approach to the teaching of e safety and through the expertise / actions of the curriculum working party.

Roles and responsibilities – pupils

Pupils:

- Are responsible for using the academy ICT systems in accordance with the pupil acceptable computer usage policy and agreement, which they will be expected to sign before being given access to academy systems. Teachers accompanying visiting pupils e.g. from within the trust, will be expected to read and understand the policy and agreement before planning the visit;
- 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 academy policies on the use of mobile phones, digital cameras and hand-held devices;
- Will be expected to know and understand academy policies on the taking/use of images and on cyber-bullying;
- Will develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- Will understand the importance of adopting good eSafety practice when using digital technologies out of academy and realise that the academy's eSafety policy covers their actions out of academy.

While 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 eSafety is therefore an essential part of the academy's eSafety provision. eSafety education will be provided in the following ways:

- A planned eSafety programme will be provided as part of ICT/PSHE/other lessons – this will include both the use of ICT and new technologies in academy and outside academy;
- Key eSafety messages will be reinforced as part of a planned programme of study;
- Pupils will be 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 will be helped to understand the need for the pupil acceptable computer usage agreement and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside academy;
- Pupils will be taught to acknowledge the source of any information used and to respect copyright when using material accessed on the internet;
- Rules for use of ICT systems/internet will be posted in all relevant rooms and displayed on log-on screens.

Roles and responsibilities – 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.

- Parents and carers will be responsible for endorsing (by signature) the pupil acceptable computer usage agreement.

Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The academy will therefore take every opportunity to help parents understand these issues through:

- Parents' evenings;
- Newsletters;
- Letters;
- Website;
- Information about all relevant national/local eSafety campaigns/literature;
- Information about useful organisations /support services for reporting eSafety issues (see appendix 2).

It is the responsibility of the parent / carer to monitor how their child's uses ICT within a home setting and in relation to home learning. Consideration should be given as to whether additional support measures are needed e.g. parental controls on home devices, shared dialogue between the child / parent about how to behave in a safe and positive when using the internet, use of only age appropriate software.

Management of infrastructure

The academy will be responsible for ensuring that the academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The academy will also ensure that the relevant people named in the above sections will be effective in carrying out their eSafety responsibilities:

- Academy ICT systems will be managed in ways that ensure that the academy meets the eSafety technical requirements outlined in the acceptable computer usage policy and any relevant national, local or trust eSafety policy and guidance;
- There will be regular reviews and audits of the safety and security of academy ICT systems;
- Servers, wireless systems and cabling will be securely located and physical access restricted;
- All users will have clearly defined access rights to academy ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually, by the eSafety committee (or other group);
- All users will be provided with a username and password by the network manager;
- The 'master/administrator' passwords for the academy ICT system, used by the network manager (or other person) are also available to the head teacher or other nominated senior leader and kept in a secure place;
- Users are made responsible for the security of their username and password must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security;
- The academy maintains and supports the managed filtering service provided by **Smoothwall**;
- Any filtering issues should be reported immediately to the network manager;
- Academy ICT technical staff regularly monitor and record the activity of users on the academy ICT systems and users are made aware of this in the acceptable computer usage policy;
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the academy systems and data;
- An agreed policy is in place in the acceptable computer usage policy regarding the downloading of executable files by users;
- Agreements are signed by members of staff in possession of academy provided laptops regarding the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other personally owned devices that may be used out of academy;
- The academy infrastructure and individual workstations are protected by up-to-date virus software;
- Personal data must not be sent over the internet or taken off the academy site unless safely encrypted or otherwise secured. See the secure data handling policy and email policy.

Curriculum

ESafety is a focus in all areas of the curriculum and staff members reinforce eSafety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches;
- Where pupils can search the internet freely, e.g. using search engines, staff are vigilant in monitoring the content of the websites the pupils visit;
- It is accepted that from time-to-time, for good educational reasons, pupils may need to research topics that might result in internet searches being blocked. In such a situation, staff

can request that the network manager temporarily removes those sites from the filtered list for the period of study. Any request to do so will be recorded, with clear reasons for the need;

- Pupils are taught in all lessons to be critically aware of the content they access on-line and are 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.

Home learning

This section of the policy will be enacted in conjunction with the academy's **Home Learning Policy**.

- The school will not regularly use live streaming as a source for teaching and learning;
- Any videos will be pre-recorded and should be checked to ensure that professional codes of conduct are adhered to and that the content is suitable for the intended audience;
- Be situated in a suitable 'public' living area within a home setting when producing video footage or completing video communication as part of a teaching resource. There will be an appropriate background – 'private' living areas within the home, such as bedrooms, are not permitted during video communication;
- Use appropriate language – this includes others in their household;
- Maintain the standard of behaviour expected in school;
- Use a work device and the necessary equipment and computer programs as intended;
- Not record, store, or distribute video material without permission;
- Ensure they have a stable connection to avoid disruption;
- Always remain aware that they are visible.

In the case of any audio communication, all colleagues and pupils must:

- Use appropriate language – this includes others in their household;
- Maintain the standard of behaviour expected in school;
- Use the necessary equipment and computer programs as intended;
- Not record, store, or distribute audio material without permission;
- Ensure they have a stable connection to avoid disruption;
- Always remain aware that they can be heard.

Using digital and video images

- When using digital images, staff inform and educate pupils about the risks associated with taking, using, sharing, publishing and distributing images. They recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Staff members are allowed to take digital/video images to support educational aims, but must follow academy policies concerning the sharing, distribution and publication of those images;
- **Any images should only be taken on academy equipment. Personal equipment of staff should *not* be used for such purposes;**
- 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. Written permission from parents or carers will be obtained.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Kept no longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Only transferred to others with adequate protection.

Staff will ensure that they comply with the secure data handling policy by:

- Taking care always to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Using personal data only on secure password protected computers and other devices, and ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data;
- Transferring data using encryption and secure password protected devices.

  Standards set out by the GDPR regulations (May 2018) should also be adhered when handling data.

Communications

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

- The official academy email service may be regarded as safe and secure and is monitored;
- Communication to parents will be through an approved channel i.e. class dojo, school email account only,
- Communication with parents will take place within the school hours where possible to ensure a work / life balance for all school staff,
- Users need to be aware that email communications may be monitored;
- Users will be expected to know and understand academy policies on email, social media (and other relevant electronic devices protocols);
- Users must immediately report, to the nominated person, in accordance with the academy policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature. Users must not respond to any such email but must follow the procedures in the email policy;
- Any digital communication must be agreed by the Head of School between staff and parents/carers or pupils. With other professional partners, both internal and external, digital communication must be professional in tone and content.

Unsuitable/inappropriate activities

Certain activities are referred to in the acceptable computer usage agreements as being inappropriate in an academy context and users must not engage in these activities in academy or outside academy when using academy equipment or systems. The academy policies on child protection, safeguarding and eSafety *must be* followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity e.g.:

- Child sexual abuse images;
- Adult material which potentially breaches the Obscene Publications Act;
- Criminally racist material;
- Other criminal conduct, activity or materials.

Should any serious eSafety incidents take place, the appropriate external authorities will be informed (e.g. local area designated safeguarding officer, police etc).

Radicalisation

The increased use of the internet due to **COVID19** has increased the opportunity for extremist groups to use the internet as a means of either inciting extremism views. Because of their personal circumstances, some young people may be susceptible to these influences.

We encourage all members of the community to report any incidents of radicalisation either directly to the police on 101, the Local Safeguarding Team at County Hall Lewes or to the school so they can action the relevant safeguarding procedures. We the school have a statutory duty to report any incidents of extremist ideology.

COVID19

As a school we acknowledge that the current health crisis has increased the need for children to access technology with greater frequency as part on an online educational platform.

At Rye Primary Community School, we advocate that children have regular breaks when accessing a screen to promote positive physical / mental wellbeing and have access to a varied curriculum which promotes practical educational experiences in addition to on line learning e.g. exercise, art/ craft activities, enrichment activities.

As a school we are happy to talk through any e-safety related queries or concerns.

Further COVID related support can be accessed from The See, Hear and Respond Partnership.

The See, Hear, Respond Partnership is a new service funded by the Department for Education. With your help, the See, Hear, Respond Partnership will quickly identify and support children, young people and families who are struggling to cope with the impacts of coronavirus.

This service can be accessed on the following website www.barnardos.org.uk.

Monitoring and reviewing

The academy will monitor the impact of the policy using:

- Logs of reported incidents;
- Monitoring logs of internet activity (i.e. ISP, academy network or managed service as appropriate);
- Internal monitoring data for network activity;
- Surveys/questionnaires of pupils, parents/carers and staff.

The policy will be reviewed by the Executive Headteacher and Advisory Council annually, or more regularly, in the light of any incidents that have taken place, significant new developments in the use of the technologies, or perceived new threats to eSafety as advised by the eSafety committee or others.

December 2021 BBL

EQUALITIES

We recognise that our pupils bring with them a wide variety of behaviours influenced by life experiences outside primary. We aim to respond to each case professionally, objectively and compassionately. We are sensitive when working with children and families with specific needs and experiences and we continuously seek ways to promote successful partnerships. The basis of differentiation will vary dependant on the needs of each case but we will consider the views of parents and families, colleagues and external agencies together with any Statement of Special Educational Need or Education, Health and Care Plan. We will also ensure compliance with the Trust's Equality Policy considering pupils with protected characteristics and making reasonable adjustments for pupils with a disability within the meaning of the Equality Act 2010. Both the primary and Trust respects the Public Sector Equality Duty (PSED) that requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. By following the Trust's Equality Policy, the primary seeks to eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by such legislation.

DATA PROTECTION

Rye Primary [The Academy] processes personal data in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All colleagues are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.

Appendix 1: Acts of Parliament Relevant to eSafety in Academies

Communications Act 2003 (section 127)

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is an offence liable, on conviction, to imprisonment. (This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.)

Computer Misuse Act 1990 (sections 1–3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- Gain access to computer files or software without permission (e.g. using someone else's password to access files).
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud).
- Impair the operation of a computer or program (e.g. caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her 'work' without permission.

The material to which copyright may attach (known in the business as 'work') must be the author's own creation and the result of some skill and judgment. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 empowers courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Criminal Justice and Immigration Act 2008 (section 63)

It is an offence to possess an 'extreme pornographic image'. An extreme pornographic image is defined in section 63 of this Act. Penalties can be up to three years' imprisonment.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and data users must comply with important data protection principles when handling personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for academies which relate to cyber-bullying/bullying:

- Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils off-site.
- Academy staff member are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the academy behaviour/anti-bullying policy.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false, or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety. This can include racist, xenophobic and homophobic comments, messages etc.

Obscene Publications Act 1959 and 1964

Publishing an 'obscene' article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows, or ought to know, that his course of conduct will cause the other so to fear on each of those occasions.

This also includes incidents of racism, xenophobia and homophobia.

Public Order Act 1986 (sections 17–29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006, it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

However, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 permit a degree of monitoring and record keeping, (e.g. to ensure communications are relevant to academy activity or to investigate or detect unauthorised use of the network.) Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as 'sexting'). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the internet). It is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Typically, teachers, social workers, health professionals, connexions staff etc fall in this category of trust. Any sexual intercourse with a child under the age of 13 commits the offence of rape.

The Data Protection Act 2018

The seven key principles of GDPR should be adhered to as stated below.

Principle (a) Lawful, fair and transparent processing

This principle emphasises transparency on how and why data is collected. You must have identified legal grounds under the GDPR (known as a "lawful basis" – of which there are six) for collecting and using personal data. You must ensure you are not in breach of other laws while processing. Personal data must be used in a way that is fair to the individuals – and you must be honest and open with individuals as to the use of their data.

Principle (b) Purpose limitation

This principle emphasises the need for organisations to be clear about what your purposes for processing are from the start. You must be clear about what your purposes for processing are from the start and these must be recorded as part of your documentation obligations (the accountability principle). You can no longer collect irrelevant information – it must serve a purpose. If a new purpose of processing arises, this data can only be used if it is compatible with the original, you gain consent, or if you have a clear basis in law.

Principle (c) Data minimisation

This principle emphasises the need for organisations to minimise the data they collect

All data collected must serve a purpose. This principle is designed to address today's digital landscape where nearly every conceivable piece of data can be collected in some way. To comply with the GDPR, organisations must only store the minimum data required.

You must ensure the personal data you are processing is:

- Adequate – sufficient to properly fulfil your stated purpose

- Relevant – has a link / is relevant to that purpose

- Limited to what is necessary – you do not hold more than you need to for that purpose.

Principle (d) Accurate and up-to-date processing

This principle requires controllers to ensure the information they hold is accurate and up-to-date and remains so. It is only lawful to use if it remains accurate and relevant. You should take all reasonable steps to ensure the personal data you hold is not incorrect or misleading in any way. If you discover that the personal data is incorrect or misleading, you must take all reasonable steps to correct or erase it as soon as possible. This principle is designed to ensure stored data is accurate and useful to the organisation using it.

Principle (e) Storage limitation

This principle emphasises the need for organisations not to keep data longer than there is a need.

Article 5(1)(e) states personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Even if you collect and use it lawfully, you cannot keep it for longer than you actually need it.

The GDPR does not set specific time limits for different types of data – this is up to you, but the retention periods you specify for the different data types should be reflected in your data retention policy.

Principle (f) Integrity and confidentiality (security)

This principle protects the integrity, privacy and confidentiality of data by placing specific obligations on organisations to secure it. Organisations who collect and process data are to be solely responsible for the security of that data, and those security measures must be wholly proportionate to the data type. To be compliant, organisations must enforce a strict data security policy that protects data from all threats.

Appendix 2: Useful services for reporting eSafety issues

Grooming or other illegal behaviour

If you want to report someone who is behaving suspiciously online towards a child, you should in an emergency contact the emergency services by calling 999, or otherwise make a report to *Child Exploitation Online Protection Centre (CEOP)*. See www.ceop.gov.uk.

Criminal content online

If you stumble across criminal content online, you should report this to the *Internet Watch Foundation (IWF)* at www.iwf.org.uk/report. Criminal content in the UK includes child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images.

On-line content which incites hatred on the grounds of race, religion and sexual orientation should be reported to *True Vision*, which tackles all forms of hate crime, including those on the grounds of disability and transgender identity. True Vision, at www.report-it.org.uk, will give you information on content which incites hatred and how to report it.

Media content inappropriate for children

If you want to make a complaint about an advert, television or radio programme, film, newspaper, magazine, video game or other type of content that you think is unsuitable for children to see or hear, you can report it through *ParentPort* at www.parentport.org.uk. Click on 'Make a Complaint' and ParentPort will take you straight to the right place to complain to.

Scams

If you have been 'scammed, ripped off or conned' you can report to *Action Fraud* on 0300 123 2040 or www.actionfraud.police.uk. This service is run by the National Fraud Authority, the UK's government agency that helps coordinate the fight against fraud.

Getting help/advice: for young people

- ChildLine: Is a free 24/7 helpline for children and young people. Visit www.childline.org.uk or call 0800 1111. ChildLine is run by the NSPCC.
- Cybermentors: For bullying issues, go on-line and talk to other children to get help and support www.cybermentors.org.uk. Cybermentors is run by Beatbullying.
- Youth 2 Youth: A young persons' helpline which offers confidential peer support via telephone, email and online chat – www.youth2youth.co.uk.
- Get Connected: A free confidential helpline for young people, open 1pm-11pm every day. Tel 0808 8084994.

Getting help/advice: for parents

- *Family Lives*: A charity providing help and support in all aspects of family life. They have a 24/7 free Parentline on 0808 8002222, or visit www.familylives.org.uk.
- *Kidscape*: Is a leading anti-bullying charity, which provides a helpline for parents of children who have been bullied. From 10am to 8pm, on 08451 205204 www.kidscape.org.uk.
- *Childnet International* Is a non-profit organisation working to help make the internet a safe place for children. 'We strive to take a balanced approach, making sure that we promote the positive opportunities, as well as responding to the risks and equipping children and young

people to deal with them'. Childnet will also offer advice on Cyberbullying. Contact details are: www.childnet.com, phone 020 7639 6967, email info@childnet.com.

Getting help/advice: for professionals working with children

- *Professionals' online safety helpline*: Helpline operated by the UK Safer Internet Centre offering professionals who work with children across the UK support, advice and mediation with on-line safety issues. The helpline can be contacted by email: helpline@saferinternet.org.uk or telephone on 0844 3814772 (calls on this number are charged at the local rate).
- *Be Internet Legends* offers access to a free internet safety curriculum with PHSE accredited lesson plans and teaching resources for Key Stage 2 pupils**.**
- *Thinkuknow* is the National Crime Agency/CEOPs education programme with age specific resources.
- *UK Safer Internet Centre* developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.
- *Educateagainsthate* provides practical advice and support on protecting children from extremism and radicalisation.

Appendix 3: Acceptable Use

By using the school's ICT network and hardware, the user agrees to abide by the Acceptable Use Agreement.

i. Acceptable Use Agreement (Summary for Primary ICT Systems)

By accepting, you agree to the terms outlined.

I will only use Primary ICT systems approved for my use e.g. computers, laptops and tablets.

I will only use email accounts approved for my use e.g. ryeprimary.co.uk.

I will not use personal emails to send and receive personal data or information.

I will not use, share or store personal data relating to pupils or staff members for non-school related activities.

I will not use, share or store personal data with pupils, staff members or third parties unless approved to do so by the Network Manager/Headteacher.

I will only use removable media approved by the Network Manager.

I will secure all school-related information stored on any removable media in line with the GDPR.

I will delete any chain letters, spam and other emails from unknown sources without opening them.

I will only access learning materials from sources approved by the Network Manager/Headteacher.

I will only access the internet for personal use outside school hours which includes break and lunch.

I will not search for, view, download, upload or transmit any explicit, inappropriate or illegal material when using the internet.

I will not use Primary ICT systems to access, download, upload, send, receive, view or display any of the following material:

- Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school;
- Content relating to a person's protected characteristics such as sexual orientation, gender assignment, religion, race, disability or age;
- Online gambling;
- Content which may adversely affect the reputation of any organisation, including the school and trust, or person, whether they are known to be true or false;
- Any sexually explicit content;
- Any other illegal content;
- Any personal data or information.

I will not share school-related passwords unless approval has been given by the Network Manager.

I will not install any software onto Primary ICT systems unless approved by the Network Manager.

[Pupils] will only use the Primary ICT systems to:

- Complete homework and coursework, and to prepare for lessons and exams;
- Undertake revision and research;
- Gather or process information for school-related or extra-curricular activities.

[Colleagues] will use, share and store personal data in line with the GDPR using encryption, where appropriate.

Reporting misuse

I will report any misuse or breaches of this agreement to the Network Manager/Headteacher.

I understand my internet use is monitored and recognise any breach of the Acceptable Use Agreement will be managed under the appropriate disciplinary policy.

I will adhere to the eSafety Policy and Acceptable Use Agreements in full.

ii. Technology acceptable use agreement – Pupils

Rye Primary understands the benefits technology can have on enhancing the curriculum and pupils' learning; however, we must ensure pupils respect primary property and use technology appropriately.

To achieve this, we have created this acceptable use agreement which outlines our expectations of pupils when using technology, whether this is on personal or primary devices, and on or off the premises.

Please read this document carefully and sign below to accept that you agree to the terms outlined.

Using technology in school

I will only use ICT systems, e.g. computers, laptops and tablets, which my classroom teacher has given me permission to use.

I will only use the approved email account that has been provided to me by the IT technician.

I will not store or use any personal data relating to a pupil or staff member for non-school related activities. If I have any queries about storing or using personal data, I will speak to my classroom teacher.

I will delete any chain letters, spam, and other emails from unknown senders without opening them.

I will ensure that I get permission from my classroom teacher before accessing learning materials, e.g. source documents, from unapproved sources.

I will only use the internet for personal use during out-of-school hours, including break and lunchtimes. During school hours, I will use the internet for school work only.

I will not share my passwords, e.g. to my school email address, with anyone.

I will not install any software onto school ICT systems unless instructed to do so by my classroom teacher.

I will only use recommended removable media, e.g. encrypted USB drives, and I will keep all school-related information stored on these secure.

I will adhere to the e-safety guidelines I have been taught.

I will only use the school's ICT facilities to:

- Complete homework and coursework, and to prepare for lessons and exams.
- Undertake revision and research.
- Gather or process information for extra-curricular activities, e.g. creating the school newsletter.

I will not use the school's ICT facilities to access, download, upload, send, receive, view or display any of the following:

- Any content that could constitute a threat, bullying or harassment, or anything negative about other persons or the school;
- Content relating to a person's protected characteristics such as sexual orientation, gender assignment, religion, race, disability or age;
- Online gambling;
- Content which may adversely affect the reputation of any organisation, including the school and trust, or person, whether they are known to be true or false;
- Any sexually explicit content;
- Any other illegal content;
- Any personal data or information.

Mobile devices

I will use school-owned mobile devices, e.g. laptops and tablets, for educational purposes only.

I will only use personal mobile devices during out-of-school hours, including break and lunchtimes, and in accordance with the Behaviour Management Policy.

I will ensure my mobile device is either switched off or set to silent mode during school hours, and will only use my device to make or receive calls when my classroom teacher permits me to do so.

I will seek permission from my classroom teacher before a school-owned mobile device is used to take images or recordings.

I will not use any mobile devices to take pictures of fellow pupils unless I have their consent.

I will not use any mobile devices to send inappropriate messages, images or recordings.

I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

I will not access the WiFi system using personal mobile devices, unless permission has been given by my classroom teacher or the IT technician.

I will not take or store images or videos of staff members on any mobile device, regardless of whether it is school-owned.

Social media

I will not use any school-owned mobile devices to access personal social networking platforms.

I will not communicate or attempt to communicate with any staff members over personal social networking platforms.

I will not accept or send 'friend requests' from/to any staff members over personal social networking platforms.

I will ensure that I apply the necessary privacy settings to any social networking sites.

I will not publish any comments or posts about the school on any social networking platforms which may affect the school's reputation.

I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.

I will not post any material online that:

- Is offensive;
- Is private or sensitive;
- Infringes copyright laws;
- Damages the school's reputation;
- Is an image or video of any staff, parent or nonconsenting pupil.

Reporting misuse

I will ensure that I report any misuse or breaches of this agreement by pupils or staff members to the headteacher.

I understand that my use of the internet will be monitored by the e-safety officer and recognise the consequences if I breach the terms of this agreement, e.g. having personal devices confiscated.

I understand that the headteacher may decide to take disciplinary action against me in accordance with the school's Behavioural Policy if I breach this agreement.

I acknowledge that I have read and understood this agreement, and ensure that I will abide by each principle.

Name:

Signed:

Date:

iii. Technology acceptable use agreement – Colleagues

Whilst Rye Primary promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, or on/off the school premises, and applies to all staff, volunteers, contractors and visitors.

Using technology in school

I will only use ICT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the headteacher.

I will only use the approved email accounts that have been provided to me.

I will not use personal emails to send and receive personal data or information.

I will not share sensitive personal data with any other pupils, staff or third parties unless explicit consent has been received.

I will ensure that any personal data is stored in line with the GDPR.

I will delete any chain letters, spam and other emails from unknown sources without opening them.

I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.

I will only use the internet for personal use during out-of-school hours, including break and lunch times.

I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.

I will not share school-related passwords with pupils, staff or third parties unless permission has been given for me to do so.

I will not install any software onto school ICT systems unless instructed to do so by the Network Manager or Headteacher.

I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.

I will only use recommended removable media and will keep this securely stored in line with the GDPR.

I will only store data on removable media or other technological devices that has been encrypted of pseudonymised.

I will only store sensitive personal data where it is necessary and which is encrypted.

I will provide removable media to the e-safety officer for safe disposal once I am finished with it.

Mobile devices

I will only use school-owned mobile devices for educational purposes.

I will only use personal mobile devices during out-of-school hours, including break and lunch times.

I will ensure that mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.

I will ensure mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.

All Pugwash staff agree to having their phone locked away in their locker at all times when within the Pugwash Nursery setting.

I will not use mobile devices to take images or videos of pupils or staff – I will seek permission from the headteacher before any school-owned mobile device is used to take images or recordings.

I will not use mobile devices to send inappropriate messages, images or recordings.

I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.

I will not access the WiFi system using personal mobile devices, unless permission has been given by the headteacher or e-safety officer.

I will not use personal and school-owned mobile devices to communicate with pupils or parents.

I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.

In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.

I will ensure that any school data stored on personal mobile devices is encrypted and pseudonymised and give permission for the e-safety officer to erase and wipe data off my device if it is lost or as part of exit procedures.

Social media and online professionalism

If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.

I will not use any school-owned mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the headteacher before accessing the site.

I will not communicate with pupils or parents over personal social networking sites.

I will not accept ‘friend requests’ from any pupils or parents over personal social networking sites.

I will ensure that I apply the necessary privacy settings to any social networking sites.

I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.

I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.

I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.

In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.

I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working at home

I will adhere to the principles of the GDPR when taking work home.

I will ensure I obtain permission from the headteacher and data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.

I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.

I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.

I will ensure my personal device has been assessed for security by the DPO and e-safety officer before it is used for lone-working.

I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.

I will act in accordance with the school's E-Security Policy when transporting school equipment and data.

Training

I will ensure I participate in any e-safety or online training offered to me, and will remain up-to-date with current developments in social media and the internet.

I will ensure that I allow the e-safety officer and DPO to undertake regular audits to identify any areas of need I may have in relation to training.

I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

I will ensure that I deliver any training to pupils as required.

Reporting misuse

I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the E-Safety Policy, e.g. to monitor pupils' internet usage.

I will ensure that I report any misuse by pupils, or by staff members breaching the procedures outlined in this agreement, to the headteacher.

I understand that my use of the internet will be monitored by the e-safety officer and recognise the consequences if I breach the terms of this agreement.

I understand that the headteacher may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Name:

Signed:

Date: