





# Online Safety Policy

<b>Policy Date:</b>	25 <sup>th</sup> September, 2023	<b>Version:</b> 1.1		
<b>Policy Review Date:</b>	September 2024	Headteacher Nitash Odedra	Signed 	Insert Date  25/09/23
<b>Ratified by Governing Body:</b>				
Sue Welford (Chair of Governors)		 Insert Signature		Insert Date  25/09/23

## **Contents**

### **1. Introduction and Overview**

- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

### **2. Education and Curriculum**

- Pupil e-safety curriculum
- Staff and governor training
- Parent awareness and training

### **3. Expected Conduct and Incident Management**

- Expected Conduct
- Social Media
- Cybercrime
- Incident Management

### **4. Managing the ICT Infrastructure**

- Internet access, security (virus protection) and filtering
- The School Website
- Network management (user access, backup, curriculum and admin)
- Photographs and video of children

### **5. Data Security**

- Management Information System access
- Data transfer

### **6. Equipment and Digital Content**

- Personal mobile phones and devices
- Digital images and video
- Asset disposal

### ***Appendices:***

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils KS1, KS2)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. What do we do if..? Guidance document.
5. Search and Confiscation guidance from DfE  
<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

## **1. Introduction and Overview**

### **Rationale**

Adapted from LGfL E-Safety Policy Revision 2015 v1 03/01/2015

**The purpose of this policy is to:**

- set out the key principles expected of all members of the school community at Rushey Mead Primary with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Rushey Mead Primary School.
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- minimise the risk of misplaced or malicious allegations made against adults who work with students.

**The main areas of risk for our school community can be summarised as follows:****Content**

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites, hate sites, incitement to extremism.
- content validation: how to check authenticity and accuracy of online content and evaluate what we see online.
- How to recognise which techniques can be used for persuasion.
- Learn how to make judgements and not make assumptions.

**Contact**

- grooming
- cyber-bullying in all forms
- identity theft (including 'fraud' (hacking Facebook profiles)) and sharing passwords
- learn that people behave different online. This can include anonymity and invisibility.

**Conduct**

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))

Adapted from LGfL E-Safety Policy Revision 2015 v1 03/01/2015

- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted inspection guidance Jan 2014)

(Ref Teaching Online safety in school – Ofsted June 2019)

## Scope

This policy applies to all members of Rushey Mead Primary School community (including staff, pupils, volunteers, parents, carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of Rushey Mead Primary School.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents or carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher / Designated Child Protection Lead	<ul style="list-style-type: none"> <li>● To take overall responsibility for Online Safety provision</li> <li>● To take overall responsibility for data and data security (SIRO)</li> <li>● To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements</li> <li>● To be responsible for ensuring that staff receive suitable training to carry out their Online Safety roles and to train other colleagues, as relevant</li> <li>● To be aware of procedures to be followed in the event of a serious e-safety incident.</li> <li>● To receive regular monitoring reports from Online Safety Coordinator</li> <li>● To ensure that there is a system in place to monitor and support staff who carry out internal Online Safety procedures (e.g. network manager)</li> <li>● To communicate regularly with SLT and the Safeguarding Governor / committee to discuss current issues, review incident logs and filtering / change control logs</li> </ul>

	<ul style="list-style-type: none"> <li>• To ensure that an Online Safety incident log is kept up to date (CPOMS)</li> <li>• Liaises with the Local Authority and relevant agencies</li> <li>• Takes day to day responsibility for Online Safety issues</li> </ul>
Online Safety Co-ordinator / Computing Lead Teacher	<ul style="list-style-type: none"> <li>• Has a leading role in establishing and reviewing the school Online Safety policies/documents</li> <li>• Promotes an awareness and commitment to Online safeguarding throughout the school community</li> <li>• Ensures that Online safety education is embedded across the curriculum</li> <li>• Liaises with school ICT technical staff</li> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident</li> <li>• Facilitates training and advice for all staff</li> <li>• Is regularly updated in Online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: <ul style="list-style-type: none"> <li>• sharing of personal data</li> <li>• access to illegal / inappropriate materials</li> <li>• inappropriate on-line contact with adults / strangers</li> <li>• potential or actual incidents of grooming</li> <li>• cyber-bullying and use of social media</li> </ul> </li> <li>• Oversees the delivery of the Online Safety element of the Computing curriculum</li> <li>• Supports with remote learning, including preparing the children for how to learn remotely and ensuring that staff adopt a duty of care relating to Online Safety</li> </ul>

Governors	<ul style="list-style-type: none"> <li>• To ensure that the school follows all current Online Safety advice to keep the children and staff safe</li> <li>• To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Safeguarding Governor</li> <li>• To support the school in encouraging parents and the wider community to become engaged in Online Safety activities</li> </ul>
Network Manager/technician	<ul style="list-style-type: none"> <li>• To report any Online Safety related issues that arises, to the e-safety coordinator.</li> <li>• To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed</li> <li>• To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date)</li> <li>• To ensure the security of the school ICT system</li> <li>• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices</li> <li>• The school's policy on web filtering is applied and updated on a regular basis</li> <li>• The LA/ web filtering provider is informed of issues relating to the filtering applied</li> <li>• That he / she keeps up to date with the school's Online Safety policy and technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant</li> </ul>

	<ul style="list-style-type: none"> <li>• That the use of the network, remote access, data systems and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Online Safety Co-ordinator /Headteacher for investigation, action or sanction.</li> <li>• To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.</li> <li>• To keep up-to-date documentation of the school's Online security and technical procedures</li> </ul>
Data Manager	<ul style="list-style-type: none"> <li>• To ensure that all data held on pupils on the school office machines have appropriate access controls in place</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>• To embed Online Safety issues in all aspects of the curriculum and other school activities</li> <li>• To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant)</li> <li>• To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws and creative commons licences.</li> </ul>

All staff	<ul style="list-style-type: none"> <li>● To read, understand and help promote the school's Online Safety policies and guidance</li> <li>● To read, understand, sign and adhere to the school staff Acceptable Use Agreement</li> <li>● To be aware of Online Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices</li> <li>● To report any suspected misuse or problem to the Head Teacher</li> <li>● To report any Online Safety issues through the school's online safeguarding platform CPOMS.</li> <li>● To maintain an awareness of current Online Safety issues and guidance e.g. through CPD</li> <li>● To model safe, responsible and professional behaviours in their own use of technology</li> <li>● To ensure that any digital communications with pupils must be on a professional level and only through school-based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.</li> </ul>
Pupils	<ul style="list-style-type: none"> <li>● Read, understand, sign and adhere to the Pupil Acceptable Use Policy</li> <li>● have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations</li> <li>● to understand the importance of reporting abuse, misuse or access to inappropriate materials</li> <li>● to know what action to take if they or someone they know feels worried or vulnerable when using online technology.</li> <li>● to know and understand school policy on the use of mobile phones, digital cameras and hand-held devices.</li> <li>● To know and understand school policy on the taking/use of images and on cyber-bullying. <ul style="list-style-type: none"> <li>● To 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</li> </ul> </li> <li>● To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home</li> <li>● to help the school in the creation/ review of Online Safety policies</li> </ul>

Parents/carers	<ul style="list-style-type: none"> <li>● to support the school in promoting Online Safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images</li> <li>● to read, understand and promote the school Pupil Acceptable Use Agreement with their children</li> <li>● to access the school websites in accordance with the relevant school Acceptable Use Agreement.</li> <li>● to consult with the school if they have any concerns about their children's use of technology</li> </ul>
External groups	<ul style="list-style-type: none"> <li>● Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school</li> </ul>



**Communication:**

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website and stored on the shared network drive
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be signed by all pupils from Years 1-6 at the start of each academic year.
- Acceptable use agreements to be signed by all members of staff as part of the Online Safety Training in the Spring term of each academic year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files.

**Handling complaints:**

- The school will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - informing parents or carers;
  - removal of Internet or computer access for a period or referral to LA / Police.
- Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Antibullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

**Review and Monitoring**

The Online Safety policy will be referenced from within other school policies: Child Protection policy, Anti-Bullying policy and Behaviour policy.

- The school has an Online Safety coordinator who will be responsible for document ownership, review and updates.
- The Online Safety policy will be reviewed regularly or when any significant changes occur with regard to the technologies in use within the school
- The Online Safety policy has been written by the school Online Safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school Online safeguarding policy will be discussed in detail with all members of teaching staff.

## 2. Education and Curriculum

### Pupil Online curriculum

This school

- Has a clear, progressive Online Safety education programme as part of the Computing curriculum as well as the PSHE curriculum, Relationships and sex education (RSE) and health. This covers a range of skills and behaviours appropriate to their age and experience.
- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind pupils about their responsibilities through an end-user Acceptable Use Policy which every pupil will sign and will be displayed throughout the school and a reminder will be displayed when a pupil logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in popups; buying on-line; on-line gaming / gambling;
- Has a whole school approach that embeds teaching about online safety and harm. In practice, this is about creating a culture that incorporates the principles of online safety across all elements of school life both outside the classroom and within the curriculum, and proactively engages staff, pupils and parents/carers. Rushey Mead Primary School promotes the agreed principles of online safety, and reviews, maintains and embeds online safety principles, as well as to model the online safety principles consistently. Classroom teachers and teaching assistants make the most of unexpected learning opportunities as they arise.
  - Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites.
  - All staff carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.
  - At Rushey Mead Primary School we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are using the cross-curricular framework 'Education for a Connected World' from UKCIS (the UK Council for Internet Safety).
  - Annual reviews of curriculum plans and learning journeys are used as an opportunity to follow this framework more closely in its key areas of Self-image and

Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

### **Staff and governor training**

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on Online Safety issues and the school's Online safety education program.
- Provides, as part of the induction process, all new staff with information and guidance on the Online safeguarding policy and the school's Acceptable Use Policies.
- Provides all staff with appropriate safeguarding and child protection training (including Online Safety, which, amongst other things, includes and understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction.
- Provides annual updated Online Safety training for all members of staff.
- Provides training that discusses technology as a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face-to-face. In many cases, abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.
- Provides training for staff that makes them aware that child on child abuse can involve consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery), upskirting which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm.

### **Parent awareness and training**

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of Online safe behaviour are made clear
  - Information in school newsletters; on the school web site;
  - suggestions for safe Internet use at home;
  - provision of information about national support sites for parents.

- o An online Safety Parent Workshop for parents which coincides with internet safety day.

### **3. Expected Conduct and Incident management**

#### **Expected conduct**

In this school, all users:

- o are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (For pupils in Nursery and Reception, it would be expected that parents/carers would sign on behalf of the pupils.)
- o need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- o need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- o must 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
- o will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They must also know and understand school policies on the taking and using images and on cyber-bullying

#### **Staff**

- o are responsible for reading the school's Online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices.

#### **Pupils**

- o must have a good understanding of research skills and acting responsibly and safely online.

#### **Parents/Carers**

- o must provide consent for pupils to use the Internet, as well as other technologies, as part of the Online Safety Acceptable Use Agreement form at time of their child's entry to the school
- o must know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

### **Social Media**

Social media (including here all apps, sites and games that allow sharing and interaction between users) is a fact of modern life, and as a school, we accept that many parents, staff and pupils will use it. However, as stated in the acceptable use policies which all members of the school community sign, we expect everybody to behave in a positive manner, engaging respectfully with the school and each other on social media, in the same way as they would face to face.

This positive behaviour can be summarised as not making any posts which are or could be construed as bullying, aggressive, rude, insulting, illegal or otherwise inappropriate, or which might bring the school or (particularly for staff) teaching profession into disrepute. This applies both to public pages and to private posts, e.g. parent chats, pages or groups.

Adapted from LGfL E-Safety Policy Revision 2015 v1 03/01/2015

- If parents have a concern about the school, we would urge them to contact us directly and in private to resolve the matter. If an issue cannot be resolved in this way, the school complaints procedure must be followed. Sharing complaints on social media is unlikely to help resolve the matter, but can cause upset to staff, pupils and parents, also undermining staff morale and the reputation of the school (which is important for the pupils we serve).
- Many social media platforms have a minimum age of 13, but the school regularly deals with issues arising on social media with pupils/students under the age of 13. We ask parents to respect age ratings on social media platforms wherever possible and not encourage or condone underage use. It is worth noting that following on from the government's Safer Internet Strategy, enforcement and age checking is likely to become more stringent over the coming years.
- However, the school has to strike a difficult balance of not encouraging underage use at the same time as needing to acknowledge reality in order to best help our pupils/students to avoid or cope with issues if they arise. Online safety lessons will look at social media and other online behaviour, how to be a good friend online and how to report bullying, misuse, intimidation or abuse. However, children will often learn most from the models of behaviour they see and experience, which will often be from adults.
- Parents can best support this by talking to their children about the apps, sites and games they use, with whom, for how long, and when (late at night / in bedrooms is not helpful for a good night's sleep and productive teaching and learning at school the next day).
- The school has an official Twitter / X account (managed by the Deputy Headteacher and Computing subject leaders) and will respond to general enquiries about the school, but asks parents/carers not to use these channels to communicate about their children.
- All members of the school community are reminded that permission is sought before uploading photographs, videos or any other information about other people.

## Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer).

Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- 'Denial of Service' (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources, and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skills and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), must consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low-level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: [Cyber Choices](#), '[NPCC- When to call the Police](#)' and [National Cyber Security Centre - NCSC.GOV.UK](#).

### **Incident Management**

In this school:

- o We refer to the *What do we do if..? Guidance document* to inform reporting pathways and appropriate responses to common Online Safety issues.
- o there is strict monitoring and application of the Online Safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- o all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- o support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with Online Safety issues
- o monitoring and reporting of Online safety incidents takes place and contribute to developments in policy and practice in e-safety within the school. The records are reviewed and audited and reported to the school's senior leaders, Governors /the LA.
- o parents / carers are specifically informed of Online safety incidents involving young people for whom they are responsible.
- o We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

## **4. Managing the ICT infrastructure**

- **Internet access, security (virus protection) and filtering**

Keeping Children Safe in Education obliges schools to "ensure appropriate filters and appropriate monitoring systems are in place and children must not be able to access harmful or inappropriate material but at the same time be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."

There are three types of appropriate monitoring identified by the Safer Internet Centre. These are:

1. Physical monitoring (adult supervision in the classroom, at all times)

Adapted from LGfL E-Safety Policy Revision 2015 v1 03/01/2015

2. Internet and web access
3. Active/Pro-active technology monitoring services

This school:

- Has the educational filtered secure broadband connectivity;
- Uses a filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network healthy through use of anti-virus software;
- Uses DfE approved methods to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal level data off-site;
- Only unblocks other external social networking sites for specific purposes;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Ensures pupils only publish within an appropriate environment
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Online Safety co-ordinator.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

#### ● **The School Website**

The school website is a key public-facing information portal for the school community (both existing and prospective stakeholders) with a key reputational value. The Headteacher/Principal and Governors have delegated has been the day-to-day responsibility of updating the content of the website to Hollie Newell (Computing Subject Leader/Online Safety lead). The site is hosted by E4Education. The DfE has determined information which must be available on a school website.

Where other staff submit information for the website, they are asked to remember:

- School have the same duty as any person or organisation to respect and uphold copyright law – schools have been fined thousands of pounds for copyright breaches.
- Where pupil work, images or videos are published on the website, their identities are protected and full names are not published.

- **Network management (user access, backup)**

This school

- Uses individual, audited log-ins for all staff users;
- Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).
- Pupils and Staff using mobile technology, where storage of data is online, will conform to the [EU data protection directive](#) where storage is hosted within the EU.

*To ensure the network is used safely, this school:*

- Ensures staff and pupils read, accept and sign the Acceptable User Policy.
- **Photographs and videos of children**
  - To comply with the Data Protection Act 1998, we ask for parents' permission before we photograph or make recordings of pupils.
  - We follow the following rules for any external use of digital images:
    - **If the pupil is named, we avoid using their photograph. If their photograph is used, we avoid naming the pupil.**
  - Where showcasing examples of pupils work, we **only** use their **first names**, rather than their full names.
  - If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.
  - Only images of pupils in suitable dress are used.

## **5. Data security: Management Information System access and Data transfer**

### **Strategic and operational practices**

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record.

We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.

- staff,
- governors,
- pupils
- parents

This makes clear staffs' responsibilities with regard to data security, passwords and access.



- We follow LA guidelines for the transfer of any data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.

### **Technical Solutions**

- Staff have secure area(s) on the network to store sensitive documents or photographs.
- We use encrypted flash drives if any member of staff has to take any sensitive information off site.
- We use VPN solution with its 2-factor authentication for remote access into our systems.
  - We store any Protect and Restricted written material in lockable storage cabinets in a lockable storage area.
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held.
- Paper based sensitive information is shredded, using cross cut shredder

## **6. Equipment and Digital Content**

### **Personal mobile phones and mobile devices**

- Mobile phones brought into school are entirely at the staff member or visitor's own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Pupils are not permitted to bring mobile phones into school.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

### **Digital images and video**

#### **In this school:**

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high-profile publications the school will obtain individual parental or pupil permission for its long-term use
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught that they must not post images or videos of others without their permission.

### **Asset disposal**

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically

destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen

- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.