James Wolfe
Primary School
with Centre for Deaf Children

Online Safety

Policy

Date written	Authorised by	Review Date
Autumn 2023	Governors	Autumn 2024

Contents

1 Introduction 3
2 Rationale 4
3 Scope 5
4 Roles and responsibilities 5
5 Communication 9
6 Handling incidents 9
7 Handling a sexting/nude selfie incident 9
8 Reviewing and monitoring online safety 10
9 Pupil online safety curriculum 11
10 Staff and governor training 11
11 Parent awareness and training 11
12 Expected conduct 11
13 Incident Management 12
14 Internet access, security (virus protection) and filtering 12
15 Network management (user access, backup) 13
16 Password policy 14
17 Email 14
18 School website 15
19 Cloud environments 15
20 Social networking 15
21 CCTV 16
22 Strategic and operational practices 16
23 Technical solutions 16
24 Mobile devices (phones, tablets and other) 16
25 Storage, syncing and access 17
26 Students' use of personal devices 17
27 Staff use of personal devices 17
28 Digital images and video 17

1 Introduction

It is our duty to ensure that every child is safe. This policy document is drawn up to protect all parties – the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

It is based on our core values:

Our children are confident learners, they work hard to succeed with every challenge.

Our children show respect for themselves and other people in our community, our country and our world.

Our children love learning and are keen to learn in our school, at home and in the future.

Our children have strong core skills in communication (reading, writing, speaking and computing), mathematics and have a good understanding of topics across the whole curriculum.

Our children are confident to share their views, listen to other people's ideas and opinions and make decisions that help everyone achieve.

And links to the following articles from the United Nations Convention on the rights of the child.

Article 18 Children have a right to be protected;

Our Online Safety Policy builds on the London Grid for Learning (LGfL) exemplar policy and should be read in conjunction with the Information Technology and Computing policy and Staff Acceptable Use Agreement.

Important note – terms filtering and monitoring.

All online access through school devices goes through internet **filtering** set by LGFL. The filtering categories are set at an appropriate level for the primary curriculum. LGFL completed the UK Safer Internet Centre audit tool assessing their service as GREEN for all measures. This can be accessed here LINK.

Online use is **monitored** through class supervision by teaching staff. Children only go online during supervised sessions.

Further information, including useful short training videos, can be accessed on the LGFL website LINK.

2 Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of our school community at with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and 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 for the whole school community.
- Have clear structures to deal with online abuse such as online bullying.
- 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
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content
- Contact
- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords
- Conduct
- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information

- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Copyright (little care or consideration for intellectual property and ownership)

3 Scope

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

4 Roles and responsibilities

Role	Key Responsibilities
Executive Headteacher with Headteacher	○ Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and relevant Local Safeguarding Children Board (LSCB) guidance ○ To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding. ○ To take overall responsibility for online safety provision ○ To take overall responsibility for data management and information security (SIRO) ensuring school's provision follows best practice in information handling ○ To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. LGfL services ○ To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles ○ To be aware of procedures to be followed in the event of a serious online safety incident ○ Ensure suitable 'risk assessments' undertaken so the curriculum meets needs of pupils, including risk of children being radicalised ○ To receive regular monitoring reports from the Online Safety Co-ordinator ○ 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

	○ To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety ○ To ensure school website includes relevant information.
Online Safety Co-ordinator and Designated Safeguarding Lead	○ Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents ○ Promote an awareness and commitment to online safety throughout the school community ○ Ensure that online safety education is embedded within the curriculum ○ Liaise with school technical staff where appropriate ○ To communicate regularly with SLT and the designated online safety Governor/committee to discuss current issues, review incident logs and filtering/change control logs ○ To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident ○ To ensure that online safety incidents are logged as a safeguarding incident ○ Facilitate training and advice for all staff ○ Oversee any pupil surveys / pupil feedback on online safety issues ○ Liaise with the Local Authority and relevant agencies ○ Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding governor (including online safety)	○ To ensure that the school has in place policies and practices to keep the children and staff safe online ○ To approve the Online Safety Policy and review the effectiveness of the policy ○ To support the school in encouraging parents and the wider community to become engaged in online safety activities ○ The role of the online safety Governor will include: regular review with the online safety Co-ordinator.
Computing Team	○ To oversee the delivery of the online safety element of the Computing curriculum

IT Technical support	○ To report online safety related issues that come to their attention, to the Online Safety Coordinator/Designated Safeguarding Lead ○ To manage the school's computer systems, ensuring: ▪ school password policy is strictly adhered to ▪ systems are in place for misuse detection and malicious attack ▪ access controls/encryption exist to protect personal and sensitive information held on school-owned devices ▪ the school's policy on web filtering is applied and updated on a regular basis ▪ That they keep 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 ▪ That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the online safety co-ordinator/Headteacher ○ To ensure appropriate backup procedures and disaster recovery plans are in place ○ To keep up-to-date documentation of the school's online security and technical procedures
Data and Information Managers	○ To ensure that the data they manage is accurate and up-to-date ○ Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. ○ The school must be registered with Information Commissioner
LGfL Nominated contacts	○ To ensure all LGfL services are managed on behalf of the school following data handling procedures as relevant
Teachers	○ To embed online safety in the curriculum ○ To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) ○ 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

All staff, volunteers and contractors.	○ To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates annually. The AUP is signed by new staff on induction. ○ To report any suspected misuse or problem to the online safety coordinator ○ To maintain an awareness of current online safety issues and guidance e.g. through CPD ○ To model safe, responsible and professional behaviours in their own use of technology **Exit strategy** ○ At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	○ Read, understand, sign and adhere to the Pupil Acceptable Use Policy annually ○ To understand the importance of reporting abuse, misuse or access to inappropriate materials ○ To know what action to take if they or someone they know feels worried or vulnerable when using online technology ○ To understand the importance of adopting safe behaviours and 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 ○ To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
Parents/carers	○ To read, understand and promote the school's Pupil Acceptable Use Agreement with their child/ren ○ to consult with the school if they have any concerns about their children's use of technology ○ to support the school in promoting online safety and agree to their children's use of the Internet at school and the school's use of photographic and video images

External groups including Parent groups	○ Any external individual/organisation will read and agree to an Acceptable Use Policy prior to using technology or the Internet within school (via guest portal on Wi-fi system) ○ to support the school in promoting online safety ○ To model safe, responsible and positive behaviours in their own use of technology.

5 Communication

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

- Policy to be posted on the school website as well as made available on the 'school' shared drive.
- Policy to be part of school induction course for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

6 Handling incidents

- The school will take all reasonable precautions to ensure online safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Online Safety Coordinator acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Online Safety Coordinator that day any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors.

7 Handling a sexting/nude selfie incident

There should always be an initial review meeting, led by the DSL. This should consider the initial evidence and aim to establish:

- Whether there is an immediate risk to a young person or young people

  When assessing the risks the following should be considered:

  - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
  - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
  - Are there any adults involved in the sharing of imagery?
  - What is the impact on the pupils involved?
  - Do the pupils involved have additional vulnerabilities?
  - Does the young person understand consent?

- Has the young person taken part in this kind of activity before?

- If a referral should be made to the police and/or children's social care
- If it is necessary to view the imagery in order to safeguard the young person – in most cases, imagery should not be viewed
- What further information is required to decide on the best response
- Whether the imagery has been shared widely and via what services and/or platforms. This may be unknown.
- Whether immediate action should be taken to delete or remove images from devices or online services
- Any relevant facts about the young people involved which would influence risk assessment
- If there is a need to contact another school, college, setting or individual
- Whether to contact parents or carers of the pupils involved - in most cases parents should be involved

An immediate referral to police and/or children's social care should be made if at this initial stage:

1. The incident involves an adult
2. There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example owing to special educational needs)
3. What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The imagery involves sexual acts and any pupil in the imagery is under 13
5. You have reason to believe a pupil or pupil is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

If none of the above apply, then a school may decide to respond to the incident without involving the police or children's social care (a school can choose to escalate the incident at any time if further information/concerns come to light).

The decision to respond to the incident without involving the police or children's social care would be made in cases when the DSL is confident that they have enough information to assess the risks to pupils involved and the risks can be managed within the school's pastoral support and disciplinary framework and if appropriate local network of support. The DSL will keep a record of the decisions made and rationale.

8 Reviewing and monitoring online safety

The online safety policy is referenced within other school policies (e.g. Safeguarding and Child Protection policy, Anti-Bullying policy).

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- 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 safety policy will be disseminated to all members of staff and pupils.

9 Pupil online safety curriculum

This school:

- has a clear, progressive online safety education programme as part of our Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience;
- plans online use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- will remind students about their responsibilities through the pupil Acceptable Use Agreements;
- ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

10 Staff and governor training

This school:

- 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 (including those on university/college placement and work experience) with information and guidance on the Online Safety Policy and the school's Acceptable Use Agreements.

11 Parent awareness and training

This school:

- provides induction for parents which includes online safety;
- runs a rolling programme of online safety advice, guidance and training for parents.

12 Expected conduct

In this school, all users:

- are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- understand it is essential to reporting abuse, misuse or access to inappropriate materials and know how to do so;
- understand the importance of adopting good online safety practice when using digital technologies in and out of school;
- know and understand school policies on the use of mobile and hand-held devices including cameras;

Staff, volunteers and contractors:

- know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers:

- should be provided information on the use of the Internet at school, as well as other technologies, as part of the school enrolment form;
- should know and understand what the school's 'rules of appropriate use for the whole school community' are and what sanctions result from misuse.

13 Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions;
- all members of the school 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;
- support is actively sought from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

14 Internet access, security (virus protection) and filtering

This school:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- ensures network health through use of Sophos anti-virus software (from LGfL) on any Windows computers;
- Uses DfE, LA or LGfL approved systems including DfE S2S and password protecting documents when emailing to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices (staff iPads are encrypted and password protected) or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;

- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

15 Network management (user access, backup)

This school:

- Uses individual, audited log-ins for all users (the LGfL USO system) for staff using desktop computers and with students when they set up their 1:1 devices
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Has daily back-up of school servers, although nearly all data is now stored via cloud computing
- Uses secure, 'Cloud' storage for data back-up that conforms to DfE guidance;
- Storage of all data within the school will conform to the EU and UK data protection requirements; Storage of data 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 read and sign that they have understood the school's online safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. The same credentials are used to access the school's network
- All pupils have their own unique username and password (USO) which gives them access to the 'London Mail' email where needed and when they are initially set up with an individual device.
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with multiple shared work area for admin staff and teaching staff. Students have no access to this resource;
- Requires all users to log off when they have finished working or lock the screen when they are leaving the computer unattended;
- Makes clear that staff are responsible for ensuring that any computer (laptop or iPad) loaned to them by the school, is used primarily to support their professional responsibilities.
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. Borough email or Intranet; finance system, Personnel system etc.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is audited and restricted and access is only through school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;

- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;

16 Password policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately.
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their passwords private.
- We require staff to use strong passwords.
- All USO Nominated Contacts are required to change their passwords every 90 days
- We require staff using critical systems to use two factor authentication.

17 Email

This school

- Provides staff with an email account for their professional use (London Staffmail) and makes clear personal email should be through a separate account;
- We use anonymous or group e-mail addresses
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
- Will ensure that email accounts are maintained and up to date
- We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos for Windows PCs, plus direct email filtering for viruses.

Pupils:

- Use the LGfL pupil email system which are intentionally ‘anonymised’ for pupil protection. This allows for the restricted sending of messages internally and externally.
- Pupils are taught about the online safety and ‘netiquette’ of using e-mail both in school and at home.

Staff:

- Staff can only use the LGfL e-mail systems on the school system
- Staff will use LGfL e-mail systems for professional purposes
- If staff or pupil personal data is transferred by email, it must be password protected first.

18 School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

19 Cloud environments

- Uploading of information on the schools' online learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the school's online environment will only be accessible by members of the school community or by a secure and unique Parent Access system;
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems. This currently is Showbie or google classroom for KS1 & KS2

20 Social networking

Staff, Volunteers and Contractors:

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.
- School staff will ensure that in private use:
    - No reference should be made in social media to students/pupils, parents/carers or school staff;
    - School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
    - They do not engage in online discussion on personal matters relating to members of the school community;
    - Personal opinions should not be attributed to the school /academy or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
    - Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.
- Students are required to sign and follow our pupil Acceptable Use Agreement each year

Parents:

- Parents are reminded about social networking risks and protocols through parent workshops on Online Safety and additional communications materials when required.
- Must not upload videos or photos that include other people's children to social media.

21 CCTV

- We do not have CCTV on our site.

22 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 have listed the information and information asset owners.
- 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 a single central record

23 Technical solutions

- Staff have access to their cloud storage (Google Drive) on the network to store sensitive files.
- We require staff to log-out or lock the screen of systems when leaving their computer.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- All servers are password protected and are managed by DBS-checked staff.
- Details of all school-owned hardware will be recorded in a hardware inventory.
- 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.
- Where any protected or restricted data has been held, we get a certificate of secure deletion for any server that once contained personal data.

24 Mobile devices (phones, tablets and other)

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.
- Only students in Years 5 and 6 are permitted to bring in their own mobile phone and only if they have permission to make their own way to and from school. This must be handed in to the class teacher at the start of the day and will be returned at the end of the day. All personal student mobile devices are stored in the office during the day.
- Staff and students are given access to school-owned mobile devices (iPads and laptops). These are the only devices to be used during lesson time.

- Videos and images should only be taken on mobile devices that the school owns. The consent of the people or person involved must always be sought.
- Staff members may use their phones during school break times.
- All visitors are requested to keep their phones on silent and not use them when around children.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying. This includes school-assigned and personal devices. Staff mobile devices may be searched at any time as part of routine monitoring.

25 Storage, syncing and access

- All school staff will be provided with a school google account that enables staff to store files in the cloud and access them remotely.

26 Students' use of personal devices

- The School strongly advises that student mobile phones and devices should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety, but this is only in Year 5 and 6.
- Mobile phones must be handed into the office at the beginning of the day and will be returned at the end of the day. They must not be turned on until the child is off the school premises.
- If a student mobile phone is found at any other time, it will be confiscated and will be held in a secure place in the school office until the end of the day.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

27 Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices in a professional capacity, such as for contacting children, young people or their families whilst at school.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes and then report the incident with the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

28 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. This is fine-grained in terms of the permissions we ask for, in line with GDPR;
- 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;
- 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;
- The school blocks/filter access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online 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 computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.