Online Safeguarding Policy

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Ouston Primary School 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 (see anti-bullying policy)
- 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 children.

The main areas of risk for our Academy 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)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

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

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students/pupils when they are off the *school/academy* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of the *school/academy*, but is linked to membership of the school/academy. 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.

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	September 2020
The implementation of this online safety policy will be monitored by the:	Online Safety Coordinator and the Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	May 2021

The school will monitor the impact of the policy using: *(delete/add as relevant)*

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
  - students/pupils
  - parents/carers
  - staff

1. Roles and Responsibilities

Head teacher-

• To take overall responsibility for e-Safety provision

• To take overall responsibility for data and data security GDPR compliant

• To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements

• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant

- To be aware of procedures to be followed in the event of a serious online safety incident.
- To receive regular monitoring reports about E-Safety from Computing Coordinator • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures.

Online Safety/Computing Co-ordinator and Designated Child Protection Lead

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies /documents
- Promotes an awareness and commitment to online safeguarding throughout the school community
- Ensures that online safety education is embedded across the curriculum
- Liaises with school COMPUTING technical staff
- To communicate regularly with SLT and the designated Online Safety Governor 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 an online safety incident log is kept up to date
- Facilitates training and advice for all staff
- Liaises 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 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 and use of social media

Governors

- To ensure that the school follows all current online safety advice to keep the children and staff safe
- To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor
- To support the school in encouraging parents and the wider community to become engaged in e-safety activities.

Computing Curriculum Co-ordinator

To oversee the delivery of the online safety element of the Computing curriculum

- To address online safety issues as they arise promptly

Network Manager/technician

The school uses third party company – Connected Its for technical support

- To report online safety related issues that come to their attention, to the Online Safety Coordinator/Designated Safeguarding Leads
- 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 (e.g. keeping virus protection up to date)

- 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/Head teacher
- 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 Protection Lead

- To take overall responsibility for data and data security
- To ensure that all data held on pupils on the school office machines have appropriate access controls in place

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

- To read, understand and help promote the school's Online Safety policies and guidance
- To read, understand, sign and adhere to the school staff Acceptable Use Policy
- 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
- 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
- To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

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
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 know and understand school policy on the use of mobile phones, digital cameras and hand held devices.
- To know and understand school policy on the taking /use of images and on cyber-bullying.
- 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

- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- To help the school in the creation/review of online safety policies

Parent and Carers

- To read, understand and promote the school’s Code of Conduct
- 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 endorse the Code of Conduct which includes the pupils’ use of the Internet and the school’s use of photographic and video images.

External groups incl. parent groups

Any external individual/organisation will sign an Acceptable Use agreement prior to using technology or the Internet within school

- To support the school in promoting online safety
- To model safe, responsible and positive behaviours in their own use of technology.

Communication

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

- Policy to be posted on the school website and posted in the staffroom.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on online safety for all staff.
- Acceptable use policy discussed with staff and pupils at the start of each year. Acceptable use policy to be issued to whole school community, on entry to the school.

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 Head teacher, unless the concern is about the Head teacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority’s Designated Officer).

Review and Monitoring

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

- The online safety policy will be reviewed every year 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 Senior Management Team and approved by Governors. All amendments to the school online safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil online safety curriculum:

- Has a clear, progressive online safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. 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 to online safety.
- 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.

Staff and governor training

Our school:

- Ensures staff and governors have had GDPR training and 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 e-safety issues, GDPR and the school's online safety education program; Termly updates in staff meetings. • 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 Safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

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

To prove support to our parents in our school:
We runs a rolling programme of advice, guidance and training for parents to ensure that principles of online safety behaviour are made clear, including: in relevant information leaflets; in school newsletters; on the school web site; through demonstrations, workshops, practical sessions held at school; suggestions for safe Internet use at home; provision of information about national support sites for parents.

Expected conduct

All users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Policy.
- 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 provide consent for pupils to use the Internet, as well as other technologies, as part of the ICT safety acceptable use agreement 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.

3. Expected Conduct and Incident Management Incident Management

In our 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, Social Care.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

Our school:

- Informs all users that Internet/email use is monitored.
- Has the educational filtered secure broadband connectivity.
- U

ses a 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 anti-virus software.
- Uses DfE or LA approved systems to send 'protect-level' (sensitive personal) data over the Internet.
- Uses encrypted devices or secure remote access where staff need to access 'protectlevel' (sensitive personal) data off-site.
- Works in partnership with Connected IT to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

Our school:

- Uses individual, audited log-ins for all staff users.
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services.
- Has additional local network monitoring/auditing software installed.
- Ensures the Technical Support Provider to be up-to-date with policies.

- Has daily back-up of school data (admin and curriculum).
- 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, our 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, username and password.
- All pupils have a distinct group username and password.
- 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 a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to log off when they have finished working or are leaving the computer unattended.
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities.
- 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 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.
- Uses secure data transfer.
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system.
- Our wireless network has been secured to appropriate standards suitable for educational use.
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Password policy

- We have made 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 has their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private.
- We require staff to change their passwords when requested.

E-mail

Our school:

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account.
- Does not publish personal e-mail addresses of staff on the school website. We use anonymous or group e-mail address, for example info@oustonprimary.org.uk for communication with the wider public.
- Any apps educational or Classroom management (Class Dojo) used by school are GDPR compliant.

- 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 systems in the school, including desktop anti-virus products, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school and at home

Staff:

- Staff can only use approved Ouston Primary School e- mail systems on the school system. • Staff will use the approved Ouston Primary School e-mail systems for professional purposes.
- Access in school to external personal e-mail accounts may be blocked.
- Never use email to transfer staff or pupil personal data. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

School website

- The Head teacher, 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.

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.
- In school, pupils are only able to upload and publish within school approved 'Cloud' systems.

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.
- The use of any school approved social networking will adhere to school's online and computing policy.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff.
- School staff should not be online friends with any pupils. Any exceptions must be approved by the Head teacher.
- 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 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.
- Pupils are required to follow online school rules.

Parents:

- Parents are reminded about social networking risks and protocols through our parental Acceptable Use Agreement and additional communications materials when required.
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer Strategic and operational practices

At our school:

- Staff are clear who are the key contact(s) for key school information.
- 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.

Technical Solutions

- We require staff to log-out of systems when leaving their computer.
- 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.
- All servers are in lockable locations and 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.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, pupils & 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.
- Mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile devices.

- No pupil within years Nursery to Year 4 should bring his or her mobile phone or personally-owned device into school (unless given permission from the Head teacher) Any device brought into school will be confiscated and returned at the end of the school day. Pupils within year 5 and 6 may bring their mobile devices into school having completed a school permission letter. Mobile phones must be handed to the class teacher on entry to the school to be kept securely locked away within the school office. No mobile phone is allowed to be used on the school premises by a pupil.
- Personal mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from Head teacher. • Pupil personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day.
- The Bluetooth or similar function of a mobile device should be switched off at all times and not be used to send images or files to other mobile devices.
- Personal mobile devices will not be used during lessons.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- Staff members may use their phones during lunch times.
- All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Head teacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Head teacher is able to withdraw or restrict authorisation for use at any time, if it is deemed necessary.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone.
- If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permission from the Head teacher to use their phone at other than lunch times.
- The School strongly advises that student mobile phones/smart watches/tablets/MP3 players should not be brought into school. The school takes no responsibility for loss or damage of any personal devices brought to school.

Storage, Synching and Access

The device is accessed with a school owned account

- The device has a school created account and all apps and file use is in line with this policy. No personal elements may be added to this device.
- PIN access to the device must always be known by the network manager.

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 within or outside of the setting.
- Staff will be issued with a school phone where contact with parents or carers is required, for instance for off-site activities.
- Mobile Phones and personally-owned devices will be switched off or switched to ‘silent’ mode. Bluetooth communication should be ‘hidden’ or switched off and 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 Head teacher /Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In our 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.
- 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, high profile use.
- 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.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

The school also has policies on :-

□ e-safety
□ Data Protection
□ Anti - Bullying
□ Acceptable use Policies
□ iPad and Laptop usage policy