Online Safety Policy

Approved by Governing Body on: 2/12/22

Signed by Chair of Governors:

Head Teacher: Amy Findlay

Date of Review: December 2023

Vision Statement

We aim to create a safe, happy and nurturing environment for all our children!

Mission Statement

The Orchard School strives to provide the best quality teaching and learning with an inclusive and personalised curriculum, where all achievements are celebrated.

Contents

1. Introduction

New technologies have become integral to the lives of children and young people today, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should always have an entitlement to safe internet access.
This policy considers the four areas of risk within online safety, which are:

- Protecting users from illegal/inappropriate/harmful content
- Protecting users from harmful online interaction/contact
- Policies for personal online behaviour/conduct
- Minimising risk from commerce

The Online Safety Policy applies to all members of the school community (including staff, children, governors, students, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

2. Rationale

This Online Safety Policy has been developed by the online safety group

It outlines the commitment of The Orchard School to safeguard members of our school community online in accordance with statutory guidance and best practice.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard children in the digital world
- describes how the school will help prepare children to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction and during training
- the Acceptable Use Agreement is to be signed by staff annually on the Safeguarding System "My Concern"

The School will deal with any incidents of inappropriate online safety behaviour related to this policy occurring in school and will, where known, inform parents/carers of incidents of that take place out of school.

3 Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, Sept 2022 and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and health education
- Searching, screening and confiscation
- It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

4 Responsibilities

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, with the support of DSL and the Governing Body, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and compliance with the policy monitored. All staff are encouraged to raise concerns as they arise with the ICT team, DSL or HT as appropriate. All visitors also receive Online Safety information on arrival at school.

The responsibility for Online Safety has been designated to a member of the senior leadership team; Barbara Ackerley (also DSL) with the support of Mark Ridgway the ICT Network and Services Manager.

Our Online Safety Coordinators ensure they keep up to date with Online Safety issues and guidance through liaison with other organisations/professionals. The school's Online Safety Coordinators ensure the Head, Senior Management and Governors are updated as necessary.

4.1 Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead/DSL
- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The headteacher is aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The headteacher is responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher/senior leaders will receive regular monitoring reports from the Online Safety Lead.

4.2 The Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.
Governors will sign an Acceptable Use of ICT agreement.

This review will be carried out by the Online safety group whose members will receive regular information about online safety incidents and monitoring reports. A nominated member of the governing body (Helen Grindulis) will take on the role of Online Safety Governor to include:

- regular meetings with the Online Safety Lead and ICT Network and Services Manager
- regularly receiving (collated and anonymised) reports of online safety incidents

- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting any concerns to the full governing body

4.3 Online Safety Lead

The Online Safety Lead will:

- work with the headteacher, ICT Network and Services Manager and other staff, as necessary, to address any online safety issues or incidents, being aware of the potential for child protection concerns
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school
- liaise with the senior head of Teaching and Learning to ensure that online safety is taught to pupils as appropriate to their age/stage of development in context.
- with the headteacher, ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- provide or identify sources of training for staff / governors / parents / carers / children
- liaise with the ICT Network and Services Manager, pastoral staff, and support staff
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- attend relevant governing body meetings/groups
- report termly to headteacher/senior leadership team.
- liaise with the local authority / or external services where appropriate.

4.3.1 Designated Safeguarding Lead (DSL)

The Designated Safeguarding Lead (who is also the online safety lead) should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

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

4.4 Curriculum Leads

Curriculum Leads will work with the Teaching and Learning Lead, with support as necessary from the Online Safety Lead, to deliver an approach to online safety education across the school day that is at the age/ stage level of children at Orchard School.

This will be provided through:

- personalised lesson planning which is age and stage appropriate.
- PHSE curriculum including relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week. (The PSHE curriculum lead is part of the online safety group.)
- Ensuring that children are monitored when using technology and safe behaviour is modelled and explicitly taught in activities and on devices as they are used.

4.5 Teaching and support staff

School staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding

- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to The Designated Safeguarding Lead or ICT Network and Services Manager for investigation/action, in line with the school safeguarding procedures
- all digital communications with children and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded where age and stage appropriate in all aspects of the curriculum and other activities
- ensure children where age and stage appropriate understand and follow the Online Safety Policy,
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource at https://swgfl.org.uk/resources/safe-remote-learning/
- they have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

4.6 The ICT Network and Services Manager

The ICT Network and Services Manager is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and other relevant polices/procedures to carry out their work effectively in line with school policy
- the school technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets (as a minimum) the required online safety technical requirements as identified by the local authority
- there is clear, safe, and managed control of user access to networks and devices
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Designated Safeguarding Lead for investigation and action. (Producing weekly Internet Monitoring Reports, that contain attempted access to sites in blocked categories related to safeguarding and any searches made that hit keywords from a list related to safeguarding)
- any concerns in reports are investigated, and reporting anything that is still a concern to the Designated Safeguarding Lead.

4.7 Children

- are supported and supervised by staff to use the school digital technology systems in accordance with the Online Safety Policy
- if cognitively able enough should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- if cognitively able enough should know what to do if they or someone they know feels vulnerable when using online technology
- if cognitively able enough should understand the importance of adopting good online safety practice when using digital technologies out of school

4.8 Parents and carers

The school will help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- publish information about appropriate use of social media relating to posts concerning the school
- requesting parents to follow Acceptable Use guidance if their child has home use of any mobile technology provided by The School and sign an agreement regarding this. (Appendix 3 below)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents will sign a relevant Acceptable Use of ICT agreement.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

4.9 Visitors including volunteers and students

Visitors, such as training providers, who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. This will sent out with the room booking

5 Acceptable use of ICT

All staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Parents will be expected to sign an agreement if their child is given any school mobile technology to use at home, and for use of images.
Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.
See appendices for Acceptable use agreements

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

- when communicating in a professional capacity, staff and others should ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and children or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses / text messaging / social media must not be used for these communications.
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and children.
- Additional software must not be downloaded onto school devices without consent (if a piece of software is required this should be discussed with the ICT Network and Services Manager)
- users should immediately report to the ICT network and services manager or online safety lead, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

The school has defined what it regards as acceptable/unacceptable use in the tables below:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	• Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					**X**
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

	Staff and other adults				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/aware pass
Online gaming	X				X			
Online shopping/commerce				X	X			
File sharing		X						X
Social media		X						X
Messaging/chat		X						X
Entertainment streaming e.g. Netflix, Disney+	X				X			
Use of video broadcasting, e.g. YouTube, Twitch, TikTok		X						X
Mobile phones may be brought to school		X			X			
Use of mobile phones for learning at school	X				X			
Use of mobile phones in social time at school			X		X			
Taking photos on mobile phones/cameras			X					X
Use of other personal devices, e.g. tablets, gaming devices			X		X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			

6 Reporting and responding

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention.
All security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the DSL or ICT Network and Services Manager.
Staff reporting an incident should log this on Myconcern.

6.1 Responding to staff actions

It is more likely that the school will need to deal with incidents that involve inappropriate /accidental rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that parents and members of the school community are aware that incidents have been dealt with.

It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary/ safeguarding procedures as follows:

The school will ensure that:

- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead / Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors (and if necessary the local authority)
- where there is no suspected illegal activity, devices may be checked using the following procedures:
    - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
    - conduct the procedure using a designated device that will not be used by children and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
    - ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
    - record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form
    - once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
        - internal response or discipline procedures
        - involvement by local authority / MAT (as relevant)
        - police involvement and/or action
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place for those reporting or affected by an online safety incident
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline (https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline); Reporting Harmful Content (https://reportharmfulcontent.com/?lang=en); CEOP (http://www.ceop.police.uk/).
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided to:
    - staff, through briefings
    - children, through assemblies/lessons (if appropriate)
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

All Incidents listed below **may** result Staff receiving a written or verbal warning, suspension or disciplinary action	Refer to line manager	Refer to Headteacher/ Principal	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		x	x	x	
Deliberate actions to breach data protection or network security rules.		x			x
Deliberately accessing or trying to access offensive or pornographic material		x	x		x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x		x
Using proxy sites or other means to subvert the school's filtering system.		x	x		x
Unauthorised downloading or uploading of files or file sharing		x			
Breaching copyright or licensing regulations.		x			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.		x			
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		x			
Using personal e-mail/social networking/messaging to carry out digital communications with childrenand parents/carers		x			
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail		x			
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner		x			
Actions which could compromise the staff member's professional standing		x			
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		x			
Failing to report incidents whether caused by deliberate or accidental actions		x			
Continued infringements of the above, following previous warnings or sanctions.		x			

6.2 Responding to Children's Actions

Children will always use technology under the visual supervision of staff. If inappropriate material (including music that contains, offensive, inappropriate or sexual language) is observed, the adult must bring that activity to an immediate end. The content should be reported to the ICT Network and Services Manager and if appropriate the DSL, who may inform parents.

7 Online Safety in the classroom

Children are taught how to use ICT responsibly within the curriculum (appropriate for their developmental level.) They are specifically taught about inappropriate use within the Relationships and Health Education curriculum.

Our children only use ICT under supervision, and do not bring personal mobile technology into school.

- Childrens needs and progress are addressed through effective planning and assessment at an appropriate developmental level.
- teaching incorporates/makes use of relevant national initiatives and opportunities e.g., Safer Internet Day and Anti-bullying week
- children are helped at their level to adopt safe and responsible ICT use
- staff should act as good role models in their use of digital technologies the internet and mobile devices

- in lessons where internet use is planned, children are guided to sites checked as suitable for their use and filtering processes are in place for dealing with any unsuitable material that is found in internet searches
- children are not allowed to freely search the internet

8 Training

8.1 Staff

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

- a planned programme of formal online safety and data protection training will be made available to all staff through National College. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation, and the need to model positive online behaviours
- the Online Safety Lead / Designated Safeguarding Lead and ICT Network and Services Manager will receive regular updates through attendance at external training events (these may be online events), (e.g. UKSIC / SWGfL / MAT / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to staff and there will be channels through which they can raise and queries
- the Online Safety Lead and ICT Network and Services Manager will provide advice/guidance/training to individuals as required.

8.2 Governors

Governors should be aware of the importance of online safety through safeguarding training and understanding this online safety policy. They should follow the acceptable use guidance in the policy. The Online Safety Governor will undertake the online safety training provided by the National College.

8.3 Families

- The School will provide parents with information on online safety as part of the Relationships and Health Education curriculum.
- There is a section on the school website in the Families section dedicated to online safety to support parents in keeping their children safe online.
- Parents will be made aware that if they have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

9 Technology

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented.
We will ensure that all staff are made aware of policy and procedures in place and explain that everyone is responsible for online safety and data protection.

9.1 Filtering

- the school filtering policies are agreed by senior leaders and technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours

- the school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
- access to online content and services is managed for all users
- illegal content (e.g., child sexual abuse images) is filtered by the broadband/filtering provider by actively employing the Internet Watch Foundation CAIC list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated
- there are established and effective routes for users to report inappropriate content
- there is a clear process in place to deal with requests for filtering changes
- the school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for staff and children)
- if at their level, our children will use child friendly/age-appropriate search engines e.g. SWGfL, Swiggle https://swiggle.org.uk/
- filtering logs are reviewed weekly and alert the school to breaches of the filtering policy, which are then acted upon.
- personal mobile devices are not allowed to access the school network..
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

9.2 Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance: (https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring) and protects users and school systems. Methods include:

- physical monitoring (adult supervision in the classroom)
- Weekly logs of reported incidents
- weekly monitoring logs of internet activity (including sites visited)
- weekly internal monitoring data for network activity
- filtering logs are analysed weekly and breaches are reported to senior leaders
- School Ipads will be audited monthly to check that no inappropriate images are stored.

The monitoring strategy for all users has been agreed and users are aware that the network is monitored. The ICT network and services manager is responsible for managing the monitoring strategy and processes. Any incidents are discussed with the online safety lead (DSL). Should serious online safety incidents take place, the Headteacher, DSL, online safety governor / chair of governors will be informed and further action will be taken through safeguarding processes or the police as necessary

9.3 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies of MIS/Financial data in the cloud
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to individual users will be determined by the ICT Network and Services Manager
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by technical staff who will keep an up-to-date record of users and their usernames

- the master account passwords for the school systems are kept in a secure place, e.g. school safe.
- passwords should be long.
- class based accounts are used for children
- The ICT Network and Services Manager is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- users should report any actual/potential technical incident/security breach to the ICT Network and Services Manager
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.
- Trainee Teachers and Long-Term Supply Staff are given their own accounts to school systems
- Short-Term Supply Staff and Visitors will be given temporary accounts if access to systems is required
- school devices are not to be used for personal use by the user or family members
- staff are forbidden from downloading executable files and installing programmes on school devices, unless they have permission from the ICT Network and Services Manager
- removable media (e.g., memory sticks/CDs/DVDs) are allowed on school devices, but must be approved and encrypted to at least FIPS 140-2 standard if they contain any personal information
- systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured.
- Any issues found will be dealt with promptly and systems updated if necessary.

10 Mobile technologies

The school acceptable use agreements for staff, children, parents, and carers outline the expectations around the use of mobile technologies.
The school allows:

	School devices			**Personal devices**		
	School owned for individual use	School owned for multiple users	Authorised device[1]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Only if a specific need has been identified	Yes	Yes
Full network access	Yes	Yes	Yes			
Internet only					Yes	Yes
No network access				Yes	Yes	Yes

10.1 School owned/provided devices:

- will be allocated to either a user or a class
- it will be agreed as to whether a device is for use in school only or if it can be used offsite
- personal use is not allowed
- levels of access to networks/internet are identified in the table above

[1] Authorised device – purchased by the learner/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- management of devices/installation of apps/changing of settings/monitoring is performed by technical staff
- technical support is provided by technical staff
- will pick up the filtering provided by the broadband provider
- access to cloud services will vary by device and users should only access their own accounts
- use on trips/events away from school is allowed for agreed devices
- data protection is provided by encryption and passwords – users should follow the Data Protection Policy
- images can be taken for educational purposes only and should be transferred to Evidence for Learning (or the school server if needed elsewhere) as soon as possible and then immediately deleted from the device
- if a user leaves the school, the device needs to be returned to technical staff who will clear the device of any user data
- users are liable for damage if they take the device offsite, including sorting any insurance they deem necessary
- staff training will be provided as necessary

10.2 Personal devices

- staff are allowed to use personal mobile devices in school, but they **must not** be used in any rooms that children have access, and must not be connected to the school network (either wired or wirelessly)
- generally, children will **not** be allowed to bring their own personal mobile devices, however, there may be an acceptation if a specific need as been identified, which will need to be approved by a member of the Senior Leadership Team
- staff may use their own devices for schoolwork or to access school systems, but must follow guidance provided by technical staff on device passwords and not saving documents to the device itself
- visitors may connect their devices to the school wi-fi for internet access only when attending a meeting or course – this connection will be subject to the same filtering and monitoring processes that occur with school devices
- no technical support is available for issues with personal devices
- management of school software licences for personally owned devices will be managed by the ICT Network and Services Manager and communicated with the relevant user
- users should follow the data protection policy
- users must not take or store any images of the school or any children
- school is not liability for loss/damage or malfunction following access to the network
- visitors will be informed about school requirements on arrival or at the start of the course/meeting

11 Social media

The school provides measures to ensure reasonable steps are in place to minimise risk of harm to children through:

- ensuring that personal information is not published
- education/training being provided regarding issues including acceptable use, social media risks, digital and video images policy, data protection
- clear reporting guidance and procedures
- guidance for children where appropriate or via parents/carers

School staff should ensure that:

- no reference is made in social media to children, parents/carers or school staff
- they do not engage in online discussion on personal matters relating to members of the school community

- personal opinions are not attributed to the school
- security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- they act as positive role models in their use of social media

Personal social media accounts

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

Any communications or content published that causes damage to the school, employees, the Local Authority, or any third party's reputation may amount to misconduct or gross misconduct and will be dealt with through the school's disciplinary policy.

School social media account

The school has a Twitter account. This is purely used to send general information which may be relevant to staff, families, and others – eg. Information about school events.
It is not used to send specific information to individual parents or staff. Email, the website, text messages or phone calls are used for this purpose.
Only the ICT Network and Servies Manager, ICT Technician, and others if they have specifically been granted permission can send messages or add Tweets to the school Twitter account

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school
- the school will respond to public social media comments made by others if appropriate and necessary
- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Cyber-bullying

Our children are unlikely to understand what cyber-bullying is, or to carry it out themselves, though they may still be exposed to it by others. They will be taught about it as developmentally appropriate within the personal, social, health education curriculum.

12 Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- Staff must be aware of those children whose images must not be taken/published.
- The personal devices of staff should not be used to take digital or video images of pupils
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take digital images of their child(ren) at school events **for their own personal use** (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some

cases protection, these images **should not be published/made publicly available** on social networking sites, nor should parents/carers comment on any activities involving other children in the digital/video images
- staff are allowed to take photographs and record images of individual children to support evidence of learning. They must follow school guidance concerning the sharing, storage, distribution, and publication of those images.
- care should be taken when sharing digital/video images that children are appropriately dressed
- photographs published on the website, or elsewhere that include children will be selected carefully and will comply with school guidance.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of children are taken for use in school or published on the school website/social media.
- parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with this policy and the school data protection policy
- images will be securely stored
- children's work can only be published with the permission of their parents/carers

13 Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media (Twitter)
- Online newsletters
- Emails and Text Messages

The school website is managed/hosted by Juniper Education. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of children, publication of school calendars and personal information – ensuring that there is least risk to members of the school community through such publications.

Where children's work, images or videos are published, their identities are protected, and full names are not published.

The school public online publishing provides information about online safety e.g., publishing the school's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc; creating an online safety page on the school website.

14 Audit and review

- An Online Safety Group comprising the ICT Network and Services Manager, online safety lead, online safety governor, PSHE lead, a parent, and the office manager, will meet twice a year to review the implementation and effectiveness of the policy.
- The *governing body* will receive an online safety report termly.
- The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place.

15 Links with other policies

This policy should be read alongside:

- Data Protection policy
- Safeguarding policy
- Staff handbook/ code of conduct
- KCSIE 2022

APPENDIX 1

Acceptable Use of Technology Agreement for Staff, Students, Visitors.

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

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, portals etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- If I access any school systems on my own device, I will ensure that the device has password/passcode protection.
- I will not download and store any school data on my own devices.
- I will only use any school issued equipment for school purposes, and I will not allow other people to use this equipment.
- I will take care to ensure that others do not have unauthorised access to school date – this includes locking devices when away from them and ensuring that I am working in such a way that others cannot view the screen.
- I will keep any portable devices that are under my responsibility locked away when I am away from them. I will not take these devices offsite unless I have permission from my Head of Department/Line Manager, in which case I will sign it out and then sign it back in on return. I will remove any unneeded photos/videos before taking the device offsite
- I will take responsibility for any school equipment issued to me. This includes protection from both theft of the information and the device itself. This includes not leaving it in an unattended vehicle.
- I understand that the school digital technology systems are primarily intended for educational use and that I will not use the systems for personal or recreational use.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it. I will ensure that all my passwords meet the complexity requirements.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Designated Safeguarding Lead or the ICT Network and Services Manager.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are

published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use official school social media accounts if I have been given permission to do so and for the reasons that I have been given permission.
- I will not use any personal social networking sites on any school owned devices.
- I will only access personal social networking sites outside of my working hours, and if on school site, only in rooms where pupils do not have access.
- I will not put my job title, the school name, or any information relating to school on my personal social networking pages.
- I will not put any information on social networking sites that may cause embarrassment to the school or bring the school into disrepute.
- I will not friend/follow/add/contact or access social networking pages of a pupil at the school, nor will I accept a request to friend/follow/add/contact a pupil.
- I will not friend/follow/add/contact or access social networking pages of parents or families of pupils or past pupils of the school, unless you are related, colleagues or you knew the person prior to the pupil starting the school. If this is the case, I will inform the designated safeguarding lead.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner. These systems include school email addresses, school telephones, web-based sites that have been setup by the school for communication (e.g. Juniper Education, Evidence for Learning), letters on school headed paper, home-school diaries. Similarly, I will not use any of these systems for personal use.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school is responsible for providing safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will only use my mobile device in rooms that pupils do not have access. If using any devices to access any school accounts, I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not connect my personal devices to any school equipment including the school's wireless network (Wi-Fi).
- I will not wear/take any wearable technology (such as smartwatches) that have a camera into the bathroom areas.
- I will not use personal email addresses on the school's ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- Where I have been informed, I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have permission from the ICT Network and Services Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or learner data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will never access any OFFICIAL information unless I have a need to do so as part of my job.
- I will never give out any OFFICIAL information via the telephone or in any other way unless I am sure who I am giving it to, that I protect it whilst in 'transit' and I have verified the entitlement of the recipient to receive it.
- I will not save any files that hold OFFICIAL information to the hard drives of any computer/laptop nor to the storage area of any tablet or handheld device; I will store such files on the school server/cloud service. I may use an approved (FIPS 140-2 certified) encrypted USB flash drive (with a secure password) if I need to transfer any files between devices, but I will not use this as a permanent data store. If a flash drive is damaged, faulty, or no longer needed, I will take this to the ICT Network and Services Manager. I will not use any unencrypted removable media for OFFICIAL information. Where technology does not allow encryption of data e.g. digital cameras and audio tapes, I will use a duty of care principle until I can move it to a secure location.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will report any data breaches immediately.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not distribute copies outside of school (including music and videos).
- I will not use any of my personal audio or video streaming accounts in school or on any school equipment, nor will I download anything from these to then use in school or on any school equipment.
- I understand that it is my responsibility to understand and follow current copyright legislation

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, dismissal, and in the event of illegal activities the involvement of the police.

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

Staff Name: ……

Signed: ……

Date: ……

Regular staff with access to MyConcern should sign the agreement on this system. It should be updated annually.

Other staff / students / visitors should give their signed forms to the Admin Office. They will be passed to the Pastoral Team to store securely, and will be updated annually

APPENDIX 2

Acceptable Use of Technology Agreement for Governors and Community Users

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

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

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

Security details:
For Governors, this form will be kept securely in the Governors Folder in a locked cupboard in school. It may be accessed by the HT, Office Manager and Governing Body if required. It will be also available to Ofsted and LA inspectors if necessary.
For Community staff the form will be kept securely by the Pastoral Team.
Forms will be kept until updated (usually annually)

Name: Signed: Date:

APPENDIX 3

Dear Parents/Carers

The General Data Protection Regulation, which replaces the Data Protection Directive 95/46/EC, which came into force on the 25th May 2018. As a result of the legislation, we have had to review how we gain consent from families.

Please complete this form detailing which activities you give your consent to and return to the school office by the as soon as possible. If you do not want to give consent for a particular activity, please indicate that you do not agree to give consent.
Consent can be withdrawn at any time.

Permission Sought	**I agree**	**I do not agree**
I give consent for school staff to take photographs of my child for recording and evidence collection. Photographs will only be used within school and shared with my family.		
School staff use anonymised evidence of pupils work (recording sheets and photographs) as part of our moderation with local special schools to ensure we are all working at similar levels. Pupils names are removed from the work and all work is returned to The Orchard School Do you give your consent for The Orchard School to share examples of work with other local schools?		
Any other professionals requesting photographs – a separate permission form will be sent out to families explaining how the images will be used and who they will be shared with.		
I give consent for school to make DVD and Video recordings of my child, to be used for recording their work as evidence. Recordings will only be used in school or shared with my family.		
I give consent for group photographs that include my child, to be used within school and shared with families of children at The Orchard School.		
I give consent for group photographs and videos that include my child, to be used within school and shared with families of children at The Orchard School via the Evidence for Learning App.		
I give consent for photographs of my child to be used on the school website. Individual children will not be named.		
I give consent for photographs of my child to appear in newspapers and magazines relating to school activities. Additional permission will be sought prior to any external photographers coming into school.		
I give consent for other families to record and photograph school productions, such as assemblies and Christmas plays. I understand my child may appear in these. All families are asked not to share any images on social media websites that feature children other than their own child.		
I give consent for my child to take part in swimming and hydrotherapy sessions.		

As part of our procedures, your child will have a routine health check; any health issues that impact on your child's inclusion in these sessions, will be discussed with school's Community Children's Nurses, who may seek advice from your child's doctor.		
I will send sunscreen into school with my child and that school staff can apply sunscreen when needed.		
If I have not sent sunscreen in, school will provide my child with school purchased cream. School staff can apply sunscreen, supplied by the school, to my child, when appropriate.		
I give consent for school to register my mobile number and email address with Juniper Education and can contact me via text message (e.g., enforced school closure due to adverse weather conditions).		
I give consent for information contained in the "All About Me" booklet, can be shared with staff at The Orchard School.		
I give consent for my child to have his/her face painted.		

Child's Name: _____ Class: _____

Signed: _____ (Parent/Guardian) Date: _____

Information provided on this sheet is protected by the provisions of the GDPR 2018. More information can be found on the school website: www.orchard.sandwell.sch.uk , within our privacy notices.

We will process the information you provide on this form in accordance with the requirements of GDPR. For further information, please see our privacy notice