



Parkside Primary School

Online Safety Policy

Reviewed September 2025

This policy is part of the School's Statutory Safeguarding Policy. Any issues and concerns with online safety must follow the school's Safeguarding and Child Protection processes.

Introduction and Overview

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Parkside 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 [noting that these need to be cross referenced with other school policies].
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance [keeping-children-safe-in-education 2025](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department'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.

The policy also takes into account the National Curriculum computing programmes of study.

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

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults;
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.
- **commerce:** being unaware of hidden costs and marketing in apps, games and websites.

Roles and responsibilities

Governors/Safeguarding governor (including online safety)

The governing board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

- To ensure that the school has in place policies and practices to keep the children and staff safe online
- To approve the Online Safety Policy and review the effectiveness of the policy
- To support the school in encouraging parents and the wider community to become engaged in online safety activities
- The role of the online safety Governor will include: regular review with the online safety Co-ordinator
- Ensure the school has reviewed protections for pupils in the home and remote-learning procedures, rules and safeguards.

Headteacher

- Must be adequately trained in off-line and online safeguarding, in-line with statutory guidance and Waltham Forest Safeguarding Board WFSCB guidance
- To lead a 'safeguarding' culture, ensuring that online safety is fully integrated with whole school safeguarding.
- To take overall responsibility for online safety provision
- To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling
- To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. London Grid for Learning (LGfL) services
- To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- To be aware of procedures to be followed in the event of a serious online safety incident
- Ensure suitable 'risk assessments' are undertaken so the curriculum meets needs of pupils, including risk of children being radicalised

- To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures.
- To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for online safety
- To ensure school website includes relevant information.

Online Safety Co-ordinator/Designated Safeguarding Lead (DSL)

- Develop an online safety culture throughout the school community as part of safeguarding
- Take day to day responsibility for online safety issues and a leading role in establishing and reviewing the school's online safety policy/documents
- Ensure that online safety education is embedded within the curriculum
- Liaise with school technical staff where appropriate
- To communicate regularly with SLT and the designated online safety Governor to discuss current issues, review incident logs and filtering reports.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- To ensure that online safety incidents are logged as a safeguarding incident
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Facilitate training and advice for all staff
- Have regular assessments of staff training in teaching and assessing the online safety elements of the curriculum
- Engage senior leaders, staff colleagues and parents in matters relating to online safety by keeping resources such as the school website, parent/carers newsletter and available training up to date
- Ensure that online safety is embedded across the whole curriculum when using ICT in different subjects
- Involve the whole school community in an annual Online Safety Day, including assemblies for each key stage and other activities throughout the day
- Keep parents and pupils informed about online safety learning resources that can be accessed outside of school.
- Regularly review guidance on the latest platforms and online risks that parents and carers need to know about - encouraging them to embed classroom learning at home and outside of school
- Oversee any pupil surveys / pupil feedback on online safety issues
- Liaise with the Local Authority and any other relevant agencies
- Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection concerns
- Work with the Headteacher and technical staff to review protections for pupils in the home and remote-learning procedures, rules and safeguards.

Computing Curriculum Leader

- To oversee the delivery of the online safety element of the Computing curriculum.
- To provide age-appropriate lesson resources and plans designed to engage young children in online safety and making learning fun, creative and memorable. Ensure plans have been designed to complement the new RSHE

curriculum and cover all the risks outlined in the UKCCIS Education for a Connected World Framework.

Computing technician

- To report online safety related issues that come to their attention, to the Online Safety Coordinator
- 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/Headteacher
- To ensure appropriate backup procedures and disaster recovery plans are in place
- To keep up-to-date documentation of the school's online security and technical procedures
- Support the Headteacher and DSL as they review protections for pupils in the home and remote-learning procedures, rules and safeguards

Data and Information - Asset Manager

- To ensure that the data they manage is accurate and up-to-date
- Ensure best practice in information management i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements.
- The school must be registered with Information Commissioner

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
- Ensure that they are aware of and adhere to safeguarding provisions for home-learning and remote-teaching technologies
- To read, understand, sign and adhere to the school staff Acceptable Use Policy (AUP), and understand any updates. The AUP is signed by new staff on induction.
- To report any suspected misuse or problem to the online safety coordinator
- To maintain an awareness of current online safety issues and guidance e.g. through CPD
- To model safe, responsible and professional behaviours in their own use of technology

Volunteers and contractors

- Read, understand, sign and adhere to an acceptable use policy (AUP)
- Report any concerns, no matter how small, to the designated safety lead / online safety coordinator
- Maintain an awareness of current online safety issues and guidance
- Model safe, responsible and professional behaviours in their own use of technology

Exit strategy

At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.

Pupils

- Read and adhere to the Pupil Acceptable Use Policy.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials
- To know what action to take if they or someone they know feels worried or vulnerable when using online technology
- To understand the importance of adopting safe behaviours and good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school
- To contribute to any 'pupil voice' / surveys that gathers information of their online experiences
- Treat home learning during any isolation/quarantine or bubble/school lockdown in the same way as regular learning in school and behave as if a teacher or parent were watching the screen

Parents/carers

- To read the school's Pupil Acceptable Use Agreement with their child/ren
- To consult with the school if they have any concerns about their children's use of technology
- To support the school in promoting online safety.
- Encourage children to engage fully in home-learning during any period of isolation/quarantine or bubble/school closure and flag any concerns
- Support the child during remote learning to ensure suitability of location; avoiding video calls in a bedroom and ensuring the child is fully dressed and not in bed, with the camera pointing away from beds/bedding/personal information etc.
- Complete the National Online Safety training for parents/carers.

External groups including 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.

How will this Policy be communicated:

- Policy will be posted on the school website.
- Regular updates and training on online safety for all staff.
- Acceptable Use Policy (AUP) is 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.
- Designated Safeguarding Leads (DSL) act as first point of contact for any incident.
- Any suspected online risk or infringement is reported to DSL / Online Safety Coordinator that day
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Handling a sexting / nude or semi-nude selfie incident:

Sexting (also known as Consensual and Non-consensual Sharing of nude and semi-nude images) involves sharing images or videos of a sexual or indecent nature that are of children (anyone under 18) or that are generated by children. It is against the law to take, make, share or possess such images. Sexting can be a form of child on child abuse.

In cases of 'sexting' the school will act in accordance with advice endorsed by DfE [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#) UKCIS 2020.

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

- Whether there is an immediate risk to a young person or young people
 - Why was the imagery shared? Was the young person coerced or put under pressure to produce the imagery?
 - Who has shared the imagery? Where has the imagery been shared? Was it shared and received with the knowledge of the pupil in the imagery?
 - Are there any adults involved in the sharing of imagery?
 - What is the impact on the pupils involved?
 - Do the pupils involved have additional vulnerabilities?
 - Does the young person understand consent?
 - Has the young person taken part in this kind of activity before?
- If a referral should be made to the police and/or children's social care

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

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

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

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

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

Pupil Online Safety Curriculum

Parkside Primary School:

- has a clear, progressive online safety education programme as part of the Computing curriculum / H(RSE) 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;
- 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;
- ensures pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff Training

All staff undertake online safety training with 'National Online Safety' (NOS) which they must revisit every year.

Governors and Parents are also encouraged to access this training.

Our DSLs/DDSLs, SENDCo and Computing Co-ordinators undertake additional training.

Expected Conduct and Incident management

In Parkside Primary School, 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 or any device with a camera built in;
- know to be vigilant in the supervision of children at all times;
- 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;

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the online 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.

Incident Management

- 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 [Child Exploitation and Online Protection command], Prevent Officer, Police, IWF [Internet Watch Foundation]) in dealing with online safety issues;
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school;
- parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law;
- we will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

Managing IT and Communication System

Internet access, security (virus protection) monitoring and filtering

Parkside Primary School:

- informs all users that Internet/email use is monitored;
- has the educational filtered secure broadband connectivity through the LGfL;
- uses the LGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- uses USO (Unified Sign-On) user-level filtering where relevant;
- ensures network health through use of Sophos anti-virus software (from LGfL);
- Uses DfE, LA or LGfL approved systems including DfE S2S (school to school), LGfL USO FX2, Egress secure file/email to send 'protect-level' (sensitive personal) data over the Internet
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management

Parkside Primary School

- Uses individual, audited log-ins for all users - the LGfL USO system;
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services;
- Uses teacher 'remote' management control tools for controlling workstations viewing users/setting-up applications and Internet web sites, where useful;

- Ensures the Systems Administrator/network manager is up-to-date with LGfL services and policies/requires the Technical Support Provider to be up-to-date with LGfL services and 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.
- Ensures staff read the school's online safety Policy. Following this, they are set-up with Internet, email and network access. Online access is through a unique, audited username and password
- Staff are responsible for keeping their password(s) private.
- 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 locking the computer if leaving it 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 school/LA approved systems:
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is audited restricted and is only through approved systems;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA or through USO secure file exchange (USO FX);
- Our wireless network has been secured to industry Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards;
- We require staff using critical systems to use two factor authentication. to ensure the network is used safely.

E-mail

Parkside Primary School

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

Staff:

- Staff will use LA or LGfL email systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- '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.
- 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 the Single Central Record.

School website

- The Headteacher, supported by the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school web site complies with statutory DfE requirements;
- 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;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students/pupils, parents/carers or school staff;
- School staff should not be online friends with any pupil/student. Any exceptions must be approved by the Headteacher.
- They do not engage in online discussion on personal matters relating to members of the school community;

- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our online safety curriculum work.

Parents:

- 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 unless requested by the police or if there is a Safeguarding issue.

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files.
- We require staff to log-out of systems when leaving their computer, but also enforce lock-out after 10 minutes idle time.
- We use the LGfL USO AutoUpdate, for creation of online user accounts for access to broadband services and the LGfL content.
- 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.
- Details of all school-owned software will be recorded in a software inventory.
- Disposal of any equipment will conform to [The Waste Electrical and Electronic Equipment Regulations 2006](#) and/or [The Waste Electrical and Electronic Equipment \(Amendment\) Regulations 2007](#). [Further information](#) can be found on the Environment Agency website.
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.
- We are using secure file deletion software.

Equipment and Digital Content

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

- Mobile devices brought into school are entirely at the staff member, students & parents or visitors own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school.

- All mobile devices brought into school by pupils must be handed in at reception.
- Staff members may use their phones during school break 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 not allowed.
- The School reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, violence or bullying.
- 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.
- 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.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity, then it will only take place when approved by the senior leadership team.
- 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 to the Headteacher / Designated Officer.
- If a member of staff breaches the school policy then disciplinary action may be taken.

The device is accessed with a personal account

- If personal accounts are used for access to a school owned mobile device, staff must be aware that school use will be synched to their personal cloud, and personal use may become visible in school and in the classroom.
- PIN access to the device must always be known by the network manager.
- Exit process – when the device is returned the staff member must log in with personal ID so that the device can be Factory Reset and cleared for reuse.

Digital images and video

- We gain parental/carers permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;
- 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.

Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints Procedures
- Acceptable Use Policy
- Computing Policy