Online Safety Policy

Date completed / last reviewed:	December 2025
Date for review:	December 2026
Cross Reference:	Anti Bullying Policy Behaviour and Discipline Policy Social Media Guidance Stivichall Safeguarding and Child Protection Policy Pupil Acceptable Use Policy Staff Acceptable Use Policy AI policy Remote Learning Policy

Learning at Stivichall is a passport for life

Introduction

National guidance continues to emphasise that it is essential for schools to take a leading role in Online Safety.

The Byron Review "Safer Children in a Digital World" stressed the role of schools:

> *"One of the strongest messages I have received during my review was about the role that schools and other services for children and families have to play in equipping children and their parents to stay safe online. To empower children and raise the skills of parents, I make recommendations to government in the following areas: delivering Online Safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area."*

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

Online safety is recognised as a key component of safeguarding under the latest keeping children safe in education (KCSIE 2025) guidance. Schools must ensure that pupils are protected from online harm through education, supervision and appropriate filtering and monitoring systems as outlined in the DfE filtering and monitoring standards (2023).

As with all of other risks, it is impossible for schools to eliminate all risks related to the use of technology. It is therefore essential, through high quality education and pastoral support, to build pupils digital resilience so they can recognise, respond to and recover from online risks effectively.

This policy is informed by national frameworks including:

Keeping Children Safe in Education (2025)

The Prevent Duty (2024)

Data Protection Act (2018) and UK GDPR

Relationship, sex and health education (RSHE) guidance

Education for a connected world (UKCIS 2023)

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

- **Content**: Being exposed to illegal, inappropriate or harmful material
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

Stivichall's online safety policy operates alongside and in conjunction with our safeguarding, data protection, behaviour and disciple, child protection, AI, anti bullying, acceptable use and curriculum policies.

The school recognises the growing importance of emerging technologies such as generative AI. Guidance for staff on the safe and ethical use of AI is incorporated in our AI policy. Online Safety and AI guidance should be considered in conjunction when planning to use AI in school.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the school relating to Online Safety:

Governors
Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about online safety and related incidents. A member of the governing body has taken on the role of online safety governor. The role of the online safety governor includes oversight of the school's compliance with the DfE filtering and monitoring standards (2023) ensuring online safety is integrated into wider safeguarding and child protection procedures and that the governing body receives annual assurance reports on the effectiveness of filtering and monitoring systems.

- Meetings with the head teacher and / or computing co-ordinator;
- Reviewing this policy on an **annual** basis;
- Ensuring their own knowledge of online safety issues is up-to-date;
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals;
- Ensuring that there are appropriate filtering and monitoring systems in place;
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers;
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified;
- Sitting on the school's Online Safety Committee (OSCOM);
- Reporting at relevant governors' meetings when necessary.
- Ensure that the school maintains compliance with the Data Protection Act 2018 and UK GDPR when using online systems, digital platforms or processing personal data.

Headteacher (DSL) and Senior Leaders:

The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community, though the day to day responsibility for Online Safety will be delegated to the computing co-ordinator.

The head teacher and senior leaders are responsible for ensuring that:

- the computing co-ordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles - and to train other colleagues;
- A system is in place to monitor Internet use effectively.
- Procedures are followed in the event of a serious online safety allegation involving staff.
- Online safety is recognised as part of the school's safeguarding responsibilities and is approached in a coordinated way.
- Safeguarding considerations are reflected in all remote learning practises.

- Detailed and secure written records of reported online safety concerns and decisions are maintained ensuring that all members of the school community understand the procedures involved in this.

The headteacher and DSLs should ensure that:

- Online safety incidents are analysed to identify trends and inform future safeguarding actions.
- The school's filtering and monitoring systems are reviewed annually and logs maintained.
- There is a clear escalation process for incidents involving potential online harm and radicalisation following the Coventry safeguarding children partnership and prevent referral pathways.

Computing Co-ordinator:

- Takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety Policy;
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place – including logging the incident on CPOMS;
- Provides training and advice for staff;
- Liaises with the Local Authority where required;
- Sits on the school's Online Safety Committee (OSCOM);
- Reports to Senior Leadership Team and governing body;
- Ensures that users may only access the school's networks through secure, password protected log-ins;
- Takes a lead role in designing the programme of study for Online Safety;
- Provides education and information for parents/carers regarding Online Safety for their children.

Designated safeguarding lead (DSL)

Should be trained in Online Safety issues and be aware of the potential for child protection issues to arise from:

- Sharing of personal data;
- Access to illegal/inappropriate materials;
- Inappropriate online contact with adults/strangers;
- Incidents of grooming;
- Cyber-bullying.

The DSL must also ensure that online safety is included in all safeguarding training for staff and that staff understand how online abuse can overlap with offline abuse. The DSL must also lead on online safety incidents where exploitation, radicalisation or sexual abuse may be factors, referring promptly to external agencies where required.

Teaching and Support Staff

Are responsible for ensuring that:

- They have awareness of Online Safety matters and the current school Online Safety policy;
- They have read, understood and signed the school staff Acceptable Use Policy (AUP);
- They report any suspected ICT misuse to the Headteacher or ICT co-ordinator promptly;
- Digital communications with pupils are kept entirely professional;
- Online Safety issues are embedded within the curriculum and other school activities;
- Pupils understand and follow the school Online Safety and Acceptable Use Policy;
- Pupils have a good understanding of research skills and the need to avoid plagiarism;
- They monitor ICT activity in lessons, extra-curricular and extended school activities;

- They understand their responsibilities relating to their personal use of social media, as laid out in the Social Media Guidance for school staff document;
- They act on incidents of cyberbullying or online harm even if these occur outside school.
- In the event of being made aware of a 'sharing of nudes and semi-nudes' type incident (formerly known as 'sexting', they inform a Designated Safeguard Lead of the incident in a timely manner, record relevant details on CPOM, and refer to UKCCIS guidance on sexting and peer on peer abuse as necessary;
- They are aware of Online Safety issues related to the use of mobile phones, wearable technologies, cameras and hand-held devices, and that they monitor their use and implement current school policies with regard to these devices.
- Promote critical thinking and resilience in pupils when engaging online and model safe digital behaviour at all times.

Pupils:

- Pupils are responsible for using the school ICT systems and Internet access safely, responsibly and lawfully. They must understand that the school's online safety and acceptable use policies are designed to keep them safe and that there will be sanctions if rules are broken. All pupils in key stage 1 and 2 are required to sign a pupil AUP before being given access to school systems;
- Pupils will understand that incidents relating to cyber-bullying and/or online safety that occur out of school, will be investigated and acted upon in school;
- Pupils will be explicitly taught through the computing, PSHE and RSHE curriculum, how to recognise, manage and report online risks including content, contact and conduct risks. They will also be supported to develop critical thinking, emotional resilience and respectful online communication in line with the education for a connected world (UKCIS 2023) framework.
- Pupils are responsible for adopting good Online Safety practice when using digital technologies out of school, and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Pupils are expected to:

- Use the Internet safely and responsibly.
- Report anything that makes them feel uncomfortable.
- Respect others when communicating online.
- Never share personal information or images inappropriately.
- Only use school approved devices and platforms within school.
- Adhere to the school's acceptable use policy.

Pupils will be encouraged to act as digital role models with digital leaders and OSCOM pupil leaders taking on an active role in peer led online safety initiatives, helping to promote safe and positive digital behaviours across the school community.

Use of Social Media and mobile technology

The school recognises that social media and mobile technology are powerful tools for communication, creativity and learning. However, they also present potential risks for misuse, reputation damage and safeguarding concerns. The use of social media and mobile technology must comply with the school's

acceptable use policies (AUPs) and safeguarding expectations. The same standard of conduct apply online as in person. Any online behaviour that may bring the school into disrepute or put pupils or staff at risk will be addressed under the relevant disciplinary and safeguarding procedures.

Staff use of social media and devices

- Staff must not use personal social media accounts to communicate with pupils or parents.
- Professional accounts should only be used for authorised school communication.
- Personal devices must not be used to capture store or share images of pupils without prior approval
- Staff should maintain strict privacy settings on personal social media accounts.
- The staff code of conduct and data protection policy apply to all online activity.
- Any personal devices used for work purposes must be password protected and where possible encrypted using 2 factor authentication.

Any misuse of social media by staff that breaches safeguarding, confidentiality or professionalism standards will be managed under the staff disciplinary and conduct policies.

Pupils' use of social media / own devices

- Pupils are not permitted to use social media during lessons unless authorised for educational purposes.
- Inappropriate or unauthorised use of personal mobile devices including taking or sharing images without consent will result in confiscation and may lead to further sanctions under the behaviour policy.
- Pupils are not permitted to bring mobile phones, smart devices or devices that have audio or visual recording capability to school without prior agreement with the head teacher. Where permission is granted, devices must be handed in at the start of the day and collected at the end.
- The school recognises that some pupils may require mobile devices for accessibility or medical reasons; These will be managed through individual risk assessments.
- Through RSHE and computing lessons, pupils will be taught about digital reputation and footprint, online consent, privacy settings and the risks of sharing content online. This includes understanding the legal implications of image sharing, cyber bullying and harassment.
- The school promotes kindness and respect online, encouraging pupils to act as digital role models and to report negative online experiences to trusted adults on their network hand.

Parents and carers use of social media

Parents and carers are expected to model positive online behaviour and respect confidentiality when posting online

- Parents should not post photographs, videos or information about other pupils on social media platforms without consent.
- The school requests that any concerns about online issues or staff conduct are raised directly with the school rather than posted publicly online.
- The school may take appropriate action including legal steps if online posts by parents cause distress harassment or reputational harm to staff or pupils.

Remote learning and online platforms

When using remote learning or communication platforms, staff must ensure that lessons, interactions and communications remain professional and comply with safeguarding and data protection expectations. On line learning environments are covered by the same behaviour standards and expectations.
Staff should only use school approved systems for communication and remote teaching. Parental consent and supervision should be encouraged for live lessons where appropriate.

- As a school, we use Seesaw as a for sending messages home, setting homework and is ready for use for home schooling if needed in the future.
- Microsoft Teams meetings should only be used where necessary in order to deliver small group sessions or 1-1 support from specialist staff. During a lockdown situation, the Teams meetings can be used to host live sessions with classes and groups of children in order to maintain effective communication and wellbeing.
- All Microsoft teams meetings with children must be approved by the Designated Safeguarding Lead.
- As a school, we must inform parents and carers of the sites that pupils/students are being asked to use, what they will be asked to do online and which members of staff they will be interacting with. During Lockdown, this has been Microsoft teams meetings, Zoom meetings and Seesaw.

- Parents evenings are completed using the school cloud and are set up in school by the digital advocate.

If the need to work remotely arises staff are asked to follow the guidance within our Remote Learning Plan.

Use of digital systems and cloud services

Staff must only use approved, secure systems for storing and sharing personal or confidential information. This includes use of school provided e-mail (Microsoft 365) and encrypted storage systems. The use of personal e-mail or personal cloud accounts for school data is strictly prohibited.
The school ensures that all third-party digital systems and software used for learning or administration are compliant with UK GDPR.

Online Safety – Preventing Radicalisation

The filtering systems used in our school blocks inappropriate content, including extremist and radicalising content.

Under The prevent duty (2024), staff must remain vigilant to signs of online radicalisation or exposure to extremist material. Where staff, children or visitors find unblocked extremist content, they must report it to a member of the Safeguarding Team, School Leadership Team or online safety lead immediately. The DSLs will follow Coventry's prevent referral pathway.

Pupils and staff should know how to report internet content that is inappropriate or of concern. Children must be given online safety education each year and have regular reminders of the use of CEOPs and online safety links on the school website.

Education – Pupils

The education of pupils in online safety at Stivichall is a vital part of the school's ICT provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience and online safety education will be provided in the following ways:

Online safety is a statutory element of safeguarding as in and is embedded across the computing, PSHE and RSHE curriculum at Stivichall Primary School. It equips pupils with the knowledge skills and confidence to use technologies safely, respectfully and responsibly- both in and beyond school.

The school also follows the education for a connected world (UKCIS 2023) framework to ensure coverage of the eight key strands of digital literacy and safety:

1. self-image and identity
2. on line relationships
3. on line reputation
4. online bullying
5. managing online information
6. health, well-being and lifestyle
7. privacy and security
8. copyright and ownership

Teachers will ensure that online safety messages are reinforced throughout all learning opportunities both in the classroom and through cross curricular projects and assemblies.

- Where pupils are allowed to search the internet (e.g. when using search engines) staff should be vigilant in monitoring the content of the websites that young people visit (the school's recommended search engine is swiggle.org.uk;

- Pupils are made aware that their activities when using school systems are being monitored and recorded, and are encouraged / taught to act responsibly when using ICT;
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a

situation, staff can request that the computing co-ordinator or Headteacher temporarily removes specific websites from the filtered list for the period of study. Any request to do so, should be presented with clear reasons for the need;

- Pupils will be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school;
- Rules for the use of ICT systems / internet will be displayed prior to children logging onto school systems;

Education -Parents / Carers

Many parents and carers have a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and can often be unsure about what they should do about it. "There is a generational digital divide". (Byron Report).
The school will take every opportunity to help parents understand relevant issues through parents' evenings, newsletters, letters, the school website, our school X (formally Twitter) feed, through our OSCom team and participation in national events such as Safer Internet Day.

The school will provide parents with signposting to age-appropriate online safety resources including the UK safer Internet centre, NCPCC online safety hub and Child Exploitation and Online Protection centre (CEOP). Guidance will also be provided on parental controls, managing screen time, social media use and supporting children with emerging technologies and AI tools.

Parents and carers are expected to model safe and respectful online behaviour when representing the school community including on social media and are encouraged to contact with the school if concerns arise.

Education & Training – Staff

It is essential that all adults working with children at Stivichall receive necessary online safety training and understand their responsibilities, as outlined in this policy. In addition, the school has taken steps towards the implementation of cyber awareness strategies for pupils and staff to ensure that they understand the basics of cyber security and protecting themselves from cybercrime. The school's cyber security strategy will be implemented in line with the DfE's 'Cyber security standards for schools and colleges'. The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Training will be offered as follows:

- All new staff with network access should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy, Acceptable Use Policy and AI Policy;
- Online safety training / CPD will be made available to staff as and when necessary;
- Staff will be given training to help them understand the issues of radicalisation, and are able to recognise the signs of vulnerability or radicalisation and know how to refer their concerns. This information also forms part of induction safeguarding training. Staff are updated as necessary in weekly staff meetings;
- The computing co-ordinator will be able to attend training sessions and review guidance documents as appropriate;
- This Online Safety Policy will be presented to, and discussed by staff in a staff meeting or INSET day as well as being shared through the national college training platform;

    - The computing co-ordinator or members of the Senior Leadership Team will provide advice / guidance / training as required to individuals.

Training – Governors

Governors should take part in online safety training / awareness sessions, with this being particularly important for those who are involved in ICT / Online Safety / health and safety / child protection. This may be offered in a number of ways, including: attendance at training provided by the Local Authority, National Governors Association or other relevant organisation; participation in school based training / information sessions for staff or parents.

Technical – Infrastructure / Equipment, Filtering and Monitoring

The school has a duty to ensure that its technical infrastructure and online environment are safe, secure and compliant with current statutory guidance.

Stivichall Primary School ensures its filtering and monitoring systems fully meet the DfE filtering and monitoring standards (2023) and the expectations of (KCSIE 2025). The governing body holds overall responsibility for ensuring that appropriate technical measures are in place and that these are reviewed regularly.

Filtering systems are designed to prevent access to harmful and inappropriate content including any material related to extremism, radicalisation, sexual abuse and self harm, while allowing educationally appropriate access. Monitoring systems provide visibility of online activity to support safeguarding and early interventions.

The school uses filtering and monitoring services recommended by the local authority and the UK safer Internet centre UK sic to ensure compliance effectiveness and proportionality.

- All users will have clearly defined access rights to school ICT systems;
- All users will be provided with a username and password for the school network. This includes teachers, teaching assistants, other designated staff and all pupils in key stages 1 and 2. A central record of all passwords used on the school systems will be kept;
- The school is currently using a filtering service provided by Impero. This blocks any sites containing banned words or which come under predetermined categories. Any attempts to access such sites, or the typing of unacceptable words, triggers a screen shot which is sent to a central log. These are then checked by SLT and IT support staff and where such screen shots require a follow up investigation, the Headteacher will be informed and incidents logged;
- Requests from staff for websites to be removed from the filtered list will be considered by the computing co-ordinator and members of the SLT. The removal, if approved, will be completed by the school IT support staff;
- The Headteacher and the computing co-ordinator can monitor the activity of users on the school ICT systems, and users are made aware of this in the Acceptable Use Policy;
- Staff are forbidden from installing programmes on school workstations / portable devices without permission from the computing Co-ordinator or Headteacher (any such installation requires administrator login;
- The school infrastructure and individual workstations are protected by up to date virus software;
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured;
- As per the Acceptable Use Policy, users may only store pupil and sensitive data on the Onedrive

Acorns Wrap Around (after school club)

Our after school provision club (Acorns) use iPads that are separate from the curriculum iPads available during school time. Acorns staff monitor these devices, and staff teach pupils to respect the devices and use them in line with our school acceptable usage policy. Acorns staff deal with any instances whereby the devices are used inappropriately (in line with our online safety policy and social media guidance policy).

Consent and Use of Digital and Video Images

The school seeks and records parental consent for the use of pupils' , video and digital recordings in line with its data protection and image use policy. Images will be used responsibly for educational purposes only and will not be shared on public platforms without explicit consent.

Staff must ensure that personal devices are not used to capture or store pupil images without prior consent from the head teacher. When images are taken from a personal device they must be removed from that device and stored on a school approved device and system as soon as possible.

- Staff will not publish any digital images of themselves, other staff or children engaged in school activities on the personal pages of social networking sites;
- Staff will ensure that their personal networking use is restricted, so that it is not publicly available;
- Staff will ensure that at all times their use of social media remains professional and does not bring the school into disrepute. This includes, but is not exclusive to, ensuring that pupils of the school do not have access to their personal sites unless there are good personal reasons that the Headteacher is aware of;
- Care should be taken when taking digital / video images of pupils, to ensure that they are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute;
- Pupils must not take, use, share, publish or distribute images of other pupils or staff without their permission;

Data Protection and GDPR

The school recognises the importance of protecting personal and sensitive information. All personal data is collected, stored, processed and shared in accordance with the Data Protection Act 2018 and the UK general data protection regulation (UK GDPR). The school acts as a data controller for the personal information of pupils, parents and staff and ensures that all processing is lawful, fair, transparent and limited to what is necessary for educational purposes.

The head teacher and the data protection officer (DPO) ensure compliance with statutory data protection requirements and the Coventry local authority data protection policy. All staff must handle data responsibly and in line with the school procedures.

Personal data shall be:

- process fairly lawfully and in a transparent manner.
- Collected for specific, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and kept up to date
- Retained only for as long as necessary.
- Process securely using appropriate technical and organisational measures.
- Only transferred to others with adequate protection.

Staff must ensure that:

- They take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- They use personal / sensitive data only on secure password protected computers and other devices;
- Personal / sensitive data is only moved or transported using secure encrypted memory sticks;
- They do not store personal or sensitive data on any non-encrypted USB stick or other device.

Staff are required to comply complete data protection and cyber security training annually. Any data breaches or suspected breaches must be reported immediately to the head teacher and the DPO and recorded in the schools data breach log.

Escalating Security Incidents e.g. remote hack, password breach

In the event of a security breach the following protocol must be adhered to:

- Report immediately to the Head teacher, on-site technician and SLT.
- Isolate and quarantine affected machine(s) – support from technician both on-site and offsite (Savvy IT, 01908 870544)
- If security incident occurs on an admin machine refer to Coventry City Council immediately (IT Service Desk 02476 786620)
- Log all incidents with Online Safety Lead including solution

Responding to Incidents of Misuse / Safeguarding

It is expected that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible misuse of ICT. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity such as:

- Child sexual abuse images;
- Criminally racist material;
- Criminal conduct, activity or materials.
- On line radicalisation or extremist content

The head teacher must be consulted with the evidence of the activity. If the evidence confirms the misuse the Headteacher has a duty to report the incident to external agencies such as the police, children's social care or the local authority prevent team.

As per safeguarding guidance – staff should not view images or videos on pupil's personal devices (see extra advice in UKCISS document, Sexting in schools and colleges).

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. The investigation should be conducted by the computing co-ordinator and the Headteacher or other member of the SLT.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and

that 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 procedures.

Further incidents that must be logged and investigated may include:

- Accessing inappropriate or illegal websites or materials.

- Using technology to harass bully or threaten others.
- Breaches of the copyright or data protection.
- Misuse of personal or social or school accounts.
- Sharing confidential information without authorisation.

Policy review, implementation and monitoring

This policy will be reviewed annually by the designated safeguarding lead the, computing coordinator and the governing body, or sooner if significant statutory or technological changes occur. The review will ensure alignment with keeping children safe in education (2025) prevent duty (2024) and the DfE filtering and monitoring standards (2023).

The DSL's and computing coordinator will monitor the effectiveness of this policy through regular analysis of incident logs, filtering and monitoring reports, staff feedback and pupil voice activities.

Any amendments or updates will be shared with all staff, governors and parents via the school website and internal communication channels.