THE ECCLESBOURNE SCHOOL

Learning Together for the Future

ONLINE SAFETY POLICY

September 2022

This policy was approved by the Trustees on the 12th of December at Full Governors

This policy will be reviewed annually on or before September 2024

This is a non-statutory policy

Contents

1 Principles of this Policy;

- This Policy outlines the commitment of The Ecclesbourne School to safeguard members of our school community online in accordance with statutory guidance and best practice. The school is aware of the legislative framework underpinning our Online Safety Policy.
- This Policy applies to all members of the school community (including staff, pupils, volunteers, 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).
- Where there is an online safety behaviour that breaches the schools expectations we will use the school behaviour policy and anti-bullying policy to inform next step actions and to the sanctions that we will put in place. Where this is the case we will inform parents and carers at the earliest opportunity.
- We will monitor the impact of the policy through logs of reported incidents, monitoring logs of internet activity (including sites visited), survey and questionnaires undertaken by staff, students and parents.
- We believe that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all pupils and staff are protected from potential harm online.
- We are aware that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- We believe that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

2 Links with statutory guidance and other policies;

This policy takes into account;

- DfE Keeping Children Safe in Education 2022
- DfE Working Together to Safeguard Children 2022
- The Derby and Derbyshire Safeguarding Children's Partnership Safeguarding procedures
- Child Protection Policy
- Anti-Bullying Policy
- Staff Code of Conduct

3 The aims of this policy is to;

- Safeguard and protect all members of The Ecclesbourne School Community online.
- Identify approaches to educate and raise awareness of online safety throughout the community.
- Enable all staff to work safely and responsibly, including in the delivery of remote learning, to role model positive behaviour online and to manage professional standards and practice when using technology.
- 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 pupils in the digital world
- Describes how the school will help prepare pupils 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 through normal communication channels this includes the staff handbook and the website
- Is published on the school website.

4 Areas of Risk

This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

5 Monitoring and Review;

Technology in this area evolves and changes rapidly. This school will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head teacher/ DSL will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report, where appropriate, to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

6 Roles and Responsibilities;

6.1 The Head Teacher and Strategic Leadership Team (SLT) will;

- The Head Teacher 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 which at this school is the Designated Safeguarding Lead.
- The Head Teacher and Designated Safeguarding Lead (DSL) are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff .
- The Head Teacher is responsible for ensuring that the DSL, 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 Head Teacher 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 Head Teacher/senior leaders will receive regular monitoring reports from the Designated Safeguarding Lead
- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including, Child Protection Policy, a staff code of conduct and Behaviour Policy
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure parents are directed to online safety advice and information
- Provide information on a school's website for parents and the community
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

[1] See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse'.

6.2 The Governing Body

The DfE guidance "Keeping Children Safe in Education 2022" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

- Trustess are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy
- This review will be carried out by the Student and Curriculum sub-committee whose members will receive regular information about online safety incidents and monitoring reports. The Safeguarding Governor will ask questions in relation to online safety in their half-termly meetings
- 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)
- Occasional review of the filtering change control logs and the monitoring of filtering logs (where possible)
- The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

6.3 The Designated Safeguarding Lead will;

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep pupils safe online.

- Access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns to the Head Teacher and Safeguarding Governor
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet termly with the safeguarding governor to discuss safeguarding concerns including online concerns
- Work with a member of the pastoral team that has responsibility for day-to-day online safety.
- Take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns.

6.4 It is the responsibility of all members of staff to;

- 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 immediately report any suspected misuse or problem to the designated safeguarding lead (DSL) for investigation/action, in line with the school safeguarding procedures
- Read and adhere to the online safety policy and acceptable use of ICT policy
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally
- Have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- Take personal responsibility for professional development in this area
- Identify students who are involved in cybercrime, or those who are technically gifted and talented and are at risk of becoming involved in cybercrime, and make a Cyber Choices referral.
- 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.

6.5 It is the responsibility of staff managing the technical environment to;

- They have an awareness of current online safety matters/trends at The Ecclesbourne School.
- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy
- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team such as passwords, encryptions and filters to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL with our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

6.6 It is the responsibility of pupils;

- Engage in age-appropriate online safety education opportunities.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

6.7 It is the responsibility of parents and carers to;

- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

7 Education and Engagement Approaches;

7.1 Education and engagement with pupils

The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst pupils by:

- Ensuring education regarding safe and responsible use precedes internet access. Including online safety in Personal, Development and Citizenship (PDC), Relationships and Sex Education (RSE) and ICT.
- Reinforcing online safety messages whenever technology or the internet is in use.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking pupil voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

7.2 Vulnerable Pupils

We recognise that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils. This could include working with the Learning Support Department and their key workers.

When implementing an appropriate online safety policy and curriculum we will seek input from specialist staff as appropriate, including the SENDCO.

7.3 Training and engagement with staff

We will:

- Provide a copy of the online safety policy via the website for staff to have access to.
- Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis, with at least annual updates. This will be through the Hays Online Training Platform.
- Cover the potential risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the community.

7.4 Awareness and engagement with parents and carers

We recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats. This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events and information evenings.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, or on the safeguarding section of the website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.

8 Concerns about pupils Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derby and Derbyshire Safeguarding Children Partnership thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

9 Unacceptable use of ICT

The following is a list, of but not exhaustive, of what the school classifies as a breach of our acceptable use of ICT statement. This is broken down into legal or illegal activity. Legal activities are referred to in section 10.9

9.1 Illegal activity

- Child sexual abuse imagery
- Child sexual abuse/exploitation/grooming
- Terrorism
- Encouraging or assisting suicide or engagement in self-harm
- 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

10 Procedures for Responding to Specific Online Incidents or Concerns

10.1 Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood "Sexual violence and sexual harassment between children in schools and colleges" guidance and part 5 of 'Keeping children safe in education'.
- The school recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
    - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- The Ecclesbourne school recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The Ecclesbourne School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PDC and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
    - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
    - If content is contained on pupils electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
    - Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
    - Implement appropriate sanctions in accordance with our behaviour policy.
    - Inform parents and carers, if appropriate, about the incident and how it is being managed.
    - If appropriate, make a referral to partner agencies, such as Children's Social Work Service and/or the Police.
    - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
        - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Kent Police first to ensure that investigations are not compromised.
    - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

10.2 Youth Produced Sexual Imagery ("Sexting")

The Ecclesbourne School recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).

- We will follow the advice as set out in the non-statutory UKCCIS guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' and KSCB guidance: "Responding to youth produced sexual imagery".
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods in our Personal Development and Citizenship Program, assemblies and ICT lessons.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using setting provided or personal equipment.

We will not:

- View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
- If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
- Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will: Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures. Ensure the DSL (or deputy) responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.

Store the device securely.

If an indecent image has been taken or shared on our network or devices, we will:

- Act to block access to all users and isolate the image.
- Carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral to Children's Social Work Service and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.

- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

10.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

The Ecclesbourne School will ensure that all members of the community are aware of online child sexual abuse, including exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.

- The Ecclesbourne School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to pupils and other members of our community. This is placed prominently on the front page of the school website.

If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- Act in accordance with our child protection policies and the relevant Kent Safeguarding Child Board's procedures.
- If appropriate, store any devices involved securely.
- Make a referral to Children's Social Work Service (if required/appropriate) and immediately inform Kent police via 101, or 999 if a child is at immediate risk.
- Carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- Inform parents/carers about the incident and how it is being managed.
- Provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.
- Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire police by using 101.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Derbyshire police using 101 unless immediate concerns and 999 will be used by the DSL (or deputy).
- If pupils at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Derbyshire Police first to ensure that potential investigations are not compromised.

10.4 10.4 Indecent Images of Children (IIOC)

The Ecclesbourne School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software. If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Derbyshire Police using 101.

If made aware of IIOC, we will:

- Act in accordance with our child protection policy and the relevant Derby City & Derbyshire Safeguarding Children Partnership Safeguarding procedures.
- Store any devices involved securely.
- Immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Derbyshire police or the LADO.

If made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Report concerns, as appropriate to parents and carers.

If made aware that indecent images of children have been found on the setting provided devices, we will:

- Ensure that the DSL (or deputy) is informed.
- Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the Derbyshire police via 101 (999 if there is an immediate risk of harm) and Children's Services using Call Derbyshire (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.

Report concerns, as appropriate to parents and carers.

If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:

- Ensure that headteacher is informed in line with our managing allegations against staff policy immediately and without any delay.
- Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
- Quarantine any devices until police advice has been sought.

10.5 Cyberbullying

Cyberbullying, along with all other forms of bullying, will not be tolerated at The Ecclesbourne School. Full details of how we will respond to cyberbullying are set out in our anti-bullying policy which must be read in conjunction with this policy.

10.6 Online Hate

Online hate content, directed towards or posted by specific members of the community will not be tolerated at The Ecclesbourne School and will be responded to in line with existing policies, including anti-bullying and behaviour.

All members of the community will be advised to report online hate in accordance with relevant policies and procedures. The Police will be contacted if a criminal offence is suspected.

If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Derbyshire police and or the safer Derbyshire website https://www.saferderbyshire.gov.uk/home.aspx

10.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site. This includes using Derbyshire's filtering system.
- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy and Derbyshire prevent pathway which may include a referral into Channel.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

10.8 Cybercrime

Cybercrime incidents and offences will be responded to in line with our existing behaviour policies. We will respond to concerns that our students are involved, or at risk of becoming involved, in cybercrime, even if it takes place off site.

Activities that might be classed as cyber-crime under the Computer Misuse At 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)

We will make a Cyber Choices referral for early intervention, as per the Cyber Choices toolkit

- If we are concerned that a child is being exploited as a result of their technical skills, we will follow the Children at Risk of Exploitation (CRE) procedure and the CRE Risk Assessment Toolkit

10.9 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 school rules)
- Promotion of any kind of discrimination
- Using school systems to run a private business
- Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Infringing copyright
- Unfair usage (downloading/uploading large files that hinders others in their use of the internet)
- 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
- Using the account of another person to access the school system
- Corrupting or destroying the data of others

11 Reporting unacceptable use of ICT

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. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents
- Reports will be dealt with as soon as is practically possible once they are received
- The Designated Safeguarding 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 the LADO.
- Where there has been a breach of the acceptable use of ICT then we will refer to the Behaviour Policy and Staff Discipline Policy for further action to be taken.

11.1 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 pupils 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
    - police involvement and/or actions
- 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 e.g., peer support for those reporting or affected by an online safety incident
- Incidents should be logged and statements taken and uploaded using My Concern
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; etc
- 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:
    - the Online Safety Group
    - staff, through regular briefings
    - pupils, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

12 Reducing Online Risks;

We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.

We will therefore;

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.

All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

13 Safer Use of Technology

13.1 Classroom Use

The Ecclesbourne School uses a wide range of technology.

This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platform/intranet
- Email
- Digital cameras, web cams and video cameras

All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place. Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.

As a school we will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community. We will ensure that the use of internet-derived materials, by staff and pupils complies with copyright law and acknowledge the source of information.

13.2 Managing Internet Access

We will maintain a written record of users who are granted access to our devices and systems. All staff, pupils and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

We will carry our regular audits and audit activity to help identify pupils trying to access sites to establish any vulnerabilities and offer advice, support and react accordingly

13.3 Filtering and Monitoring

When considering filtering and monitoring we will refer to 'A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring

13.4 Decision Making

The school leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit pupil's exposure to online risks.

The leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding. Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded. The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard pupils; effective classroom management and regular education about safe and responsible use is essential.

If pupils discover unsuitable sites, they will be required to report it to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff. The breach will be recorded and escalated as appropriate. Parents/carers will be informed of filtering breaches involving their child.

Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Derbyshire Police or CEOP.

We will appropriately monitor internet use on all setting owned or provided internet enabled devices.

13.5 Security and Management of Information Systems

We take appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly.
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
- Specific user logins and passwords will be enforced for all.

All users are expected to log off or lock their screens/devices if systems are unattended.

13.6 Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

If using online recording systems for example My Concern to report Child Protection concerns, restricted access will be granted per job role and responsibility with regular reviews of who has access

When students join the school in Year 7 they are provided with their own unique username and private passwords to access our systems; pupils are responsible for keeping their password private.

We require all users to:

- Use strong passwords for access into our system - the longer and more unusual, the stronger it becomes. Using a combination of upper, lower case, numbers and special characters is recommended.
- Change their passwords when prompted to do so
- Always keep their password private; users must not share it with others or leave it where others can find it.
- Not to login as another user at any time.

13.7 Managing the Safety of our Website

We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE) and compliance checks are carried out on a regular basis.

We will ensure that our website complies with guidelines for publications including:

- Accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or pupil's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

13.8 Publishing Images and Videos Online

We will ensure that all images and videos shared online are used in accordance with the associated polices and parental permission.

13.9 Managing Email

Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the staff code of conduct policy.

- The forwarding of any chain messages/emails is not permitted.
- Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
- Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell the Designated Safeguarding Lead if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by the DSL.

13.10 Staff email

Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, pupils and parents.

Members of staff will refer to and adhere to the acceptable use policy and any other policy where staff use of mobiles is referred to.

13.11 Pupil email

Pupils will use provided email accounts for educational purposes. Pupils will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

13.12 Educational use of Videoconferencing and/or Webcams

We recognise that videoconferencing and/or use of webcams can be a challenging activity but brings a wide range of learning benefits.

- All videoconferencing and/or webcam equipment will be switched off when not in use and will not be set to auto-answer.

- Video conferencing equipment connected to the educational broadband network will use the national E.164 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
- Videoconferencing contact details will not be posted publicly.
- Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.
- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

14 Management of Applications (apps) used to Record Children's Progress

We use SIMS to track pupils progress and share appropriate information with parents and carers.

The Head Teacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.

To safeguard pupil's data:

- Only pupil issued devices will be used for apps that record and store pupils' personal details, attainment or photographs.
- Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store pupils' personal details, attainment or images.
- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

15 Social Media

15.1 Expectations

The expectations' regarding safe and responsible use of social media and remote learning platforms applies to all members of The Ecclesbourne School Community.

Members of staff will refer to and adhere to the schools staff code of conduct policy and any other policy where the staff use of social media is referred to. We will control pupil and staff access to social media whilst using setting provided devices and systems on site.

Concerns regarding the online conduct of any member of The Ecclesbourne School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

15.2 Pupils Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources. We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for pupils under this age.

Any concerns regarding pupil's use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

- Pupils will be advised in their taught To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
- To use safe passwords.
- To use social media sites which are appropriate for their age and abilities.
- How to block and report unwanted communications.
- How to report concerns both within the setting and externally.

16 Use of Personal Devices and Mobile Phones

The Ecclesbourne School recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.

16.1 Staff Use of Personal Devices and Mobile Phones

Members of staff will refer to and adhere to the schools acceptable use of ICT policy and the staff code of conduct.

16.2 Pupils Use of Personal Devices and Mobile Phones

Pupils from Years 7- 11 are not to bring their mobile phone into school and a range of sanctions are put in place if they do so as per our behaviour policy. Sixth Formers are able to bring their phones into school but they must only be used in the Sixth From Centre or in lessons as directed by the teacher. Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examination as per the sanctions issued by the relevant examination board.

Staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting). Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy www.gov.uk/government/publications/searching-screening-and-confiscation

Pupils mobile phones or devices may be searched by a member of the senior leadership team, with the consent of the pupil or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies. www.gov.uk/government/publications/searching-screening-and-confiscation

Mobile phones and devices that have been confiscated will be released to parents or carers as prescribed by the sanction that has been put in place.

If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

16.3 Visitors' Use of Personal Devices and Mobile Phones

Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.

We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or headteacher of any breaches our policy.

16.4 Officially provided mobile phones and devices.

Members of staff will be issued with a work phone number and email address, where contact with pupils or parents/ carers is required.

Setting mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

17 Useful Links for Educational Settings

Support and Guidance for Educational Settings

Derby City & Derbyshire Safeguarding Children Partnership on line procedures DDCSP:

- **http://derbyshirescbs.proceduresonline.com/**

Derbyshire Police:

In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact Derbyshire Police via 101

LADO

- By referral into Professional.Allegations@derbyshire.gov.uk
- Form found here http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

- Immediate risk of harm phone 01629 533190
- For all other referrals complete an online form https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx
- For professional advice phone 01629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
    - www.thinkuknow.co.uk
    - www.ceop.police.uk

    - Childnet: www.childnet.com
    - Get Safe Online: www.getsafeonline.org
    - Internet Matters: www.internetmatters.org
    - Internet Watch Foundation (IWF): www.iwf.org.uk
    - Lucy Faithfull Foundation: www.lucyfaithfull.org
    - NSPCC: www.nspcc.org.uk/onlinesafety
        - ChildLine: www.childline.org.uk
        - Net Aware: www.net-aware.org.uk
    - The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
    - UK Safer Internet Centre: www.saferinternet.org.uk

Signed by:

Chair of Trustees..... Head Teacher .....

Date: