Online Safety

Policy

‘Together we unlock potential and learn for life’

This policy was approved by the Governing Body of Moor First School at their meeting on:

Signed …………………………………..Chair of Governors

Signed …………………………………Safeguarding governor

Signed …………………………………..Headteacher

Review Frequency: Every 3 years Next Review: January 2028

Aims:

Our school aims to:

➢ Have robust processes in place to ensure the online safety of children, staff, volunteers, and governors.

➢ Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology

➢ Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:
Content – being exposed to illegal, inappropriate, or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, and extremism.
Contact – being subjected to harmful online interaction with other users, such as peer-to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending, and receiving explicit images (e.g., consensual, and nonconsensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and guidance

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

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.
It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyberbullying by, if necessary, searching for and deleting inappropriate images or files on children's electronic devices where they believe there is a 'good reason' to do so.
The policy also considers the National Curriculum computing programmes of study.

Our School

Access to IT facilities, the internet and social media must be in support of educational activities and appropriate to the aims of the school. The aims of this policy and agreements is to ensure that all pupils and staff are clear about what constitutes appropriate use of technology, the internet and social media, within the school and when using school IT resource and that all users are aware of the possible consequences of inappropriate use, which could include temporary or permanent loss of access to computing facilities, or even result in serious disciplinary action being taken. Misuse of technology from the age of ten upwards can result in legal prosecution and charges.

All pupils and staff, who access the internet or social media from the school site or using school technology resources when off site, must be aware that they are responsible for everything that takes place on their computers, tablets or mobile phones and that all activity, including use of the internet may be logged.

BENEFITS

Access to the internet, email and social media will enable pupils and staff to:

- Access and explore a wide variety of sources of information to support and enhance the educational experience
- Access curriculum resources and exchange work with staff and other pupils
- Access webinars, videos and other resources to support the curriculum
- Keep informed of news and current events
- Take part in live discussions and other events
- Extend the curriculum and be included in initiatives relevant to their education and take part in global educational projects
- Make links with experts
- Publish and display work via websites
- Communicate with other internet users around the world

EFFECTIVE USE

Internet and social media access will be planned to enrich and extend learning. Pupils will make best use of the internet and social media if:

- They have been given clear objectives for using the internet and social media.
- They have been educated in safe, responsible and effective internet or social media use.
- They are supervised when appropriate.
- They appreciate and control their internet use, ensuring that they balance learning and they understand and apply safeguarding principles, how to handle themselves safely on-line and how and where to report any Child Exploitation, On-line Protection, counter-terrorism and radicalisation issues.
- They are encouraged to evaluate sources and to discriminate between valid and inappropriate materials.
- They know how to copy, save and edit material from the internet or social media without infringing copyright and data protection.

RESPONSIBILITIES

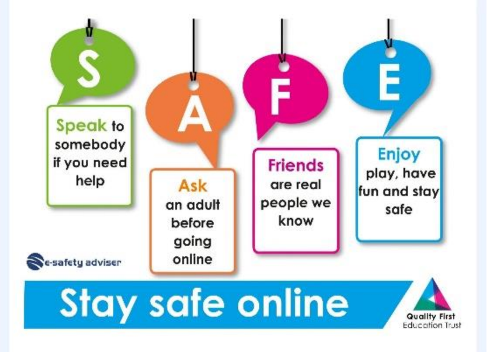
As e-safety is an important aspect of strategic leadership within the school, the Governing Body have ultimate responsibility to ensure that policy and practices are embedded and monitored. The responsibility is delegated to the Headteacher. Any extra permission given by the Headteacher must be recorded (memos, minutes from meetings) in order to be validated.

The Headteacher (Designated Safeguarding Lead) and Deputy Safeguarding Lead, have responsibility for ensuring that all members of the school community uphold this policy and they have been made aware of the implication that this has. It is the role of these members of staff to keep abreast of new guidance such as the LA, CEOP, Childnet and Local Authority Safeguarding Children Board.

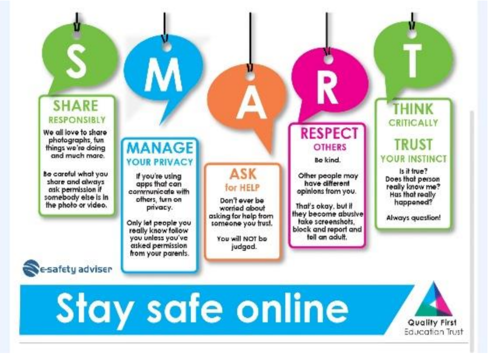
As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are required to read and sign the Acceptable Use Policy.

It is the pupil's responsibility to use these resources in a manner that is efficient, ethical and legal. They are required to **read and sign the Acceptable Use Policy.** All children will engage in a discussion about this with their teacher to ensure that they fully understand. The use of computing resources is a privilege and therefore, inappropriate use may result in this being withdrawn.

E-safety rules will be posted in classrooms and safer internet day celebrated in school.
KS1 poster:


S
A
F
E
Speak to somebody if you need help
Ask an adult before going online
Friends are real people we know
Enjoy play, have fun and stay safe
e-safety adviser
Stay safe online
Quality First Education Trust

KS2 poster:



S

SHARE RESPONSIBLY

We all love to share photographs, fun things we're doing and much more.

Be careful what you share and always ask permission if somebody else is in the photo or video.

M

MANAGE YOUR PRIVACY

If you're using apps that can communicate with others, turn on privacy.

Only let people you really know follow you unless you've asked permission from your parents.

A

ASK for HELP

Don't ever be worried about asking for help from someone you trust.

You will NOT be judged.

R

RESPECT OTHERS

Be kind.

Other people may have different opinions from you.

That's okay, but if they become abusive take screenshots, block and report and tell an adult.

T

THINK CRITICALLY

TRUST YOUR INSTINCT

Is it true? Does that person really know me? Has that really happened?

Always question!

e-safety adviser

Stay safe online

Quality First Education Trust

We also use Project Evolve teaching resources and Purple Mash scheme of work to teach online safety through a progressive curriculum.

DATA SECURITY AND PRIVACY

All data is stored in accordance with provision of the General Data Protection Regulations.

SAFETY, SOCIAL MEDIA PLATFORMS, LEARNING PLATFORMS AND REPORTING MISUSE

Internet access from the school site is carefully filtered and monitored. Access to inappropriate websites will be blocked, either on a website-by-website basis or by blocking inappropriate key images, words or phrases. Internet activity on the school premises is monitored and logged via Securus. School technology equipment used off site may be checked for inappropriate use. In the case of tablets, pupils, parents and staff have a responsibility to act in accordance with the policy and associated guidance. Appropriate sanctions are in place and will be carried out in the event of misuse.

Staff must obtain permission from Senior Leaders to use any chat room services. Live chat rooms must not be used unless posts are filtered prior to posting.

Social media

The authorised social media platforms available to Moor First are solely X (formerly Twitter) and Facebook. These platforms can be used by school to celebrate achievements and promote news across the whole school.

Staff must not use any existing personal social media accounts for school social media activity. Staff must only use the school accounts for school social media and the Headteacher/Secretary create the posts to ensure that safeguarding standards are upheld.

It is ultimately the responsibility of staff to ensure that they set and convey appropriate standards for social media and internet use. Staff and pupils should be aware at all times of the potential consequences of inappropriate use of the internet or social media, which could include loss of access to school computing facilities, disciplinary action and, in extreme cases where misuse could constitute a criminal offence (for example, an incident of cyberbullying, exchanging indecent images, accessing extreme pornography or extremist/radicalisation material) will be reported to the appropriate police or other child protection authority.

Staff should not befriend pupils or their families on social media unless they are related to them.

Any pupil who suspects misuse of the internet, social media or computing facilities by another pupil must report this to their classroom teacher. Any member or staff who suspects misuse of the internet, social media or computing facilities must report this to the Headteacher. Any serious or potentially illegal misuse of the internet or computing facilities such as accessing pornography, cyber-bullying and on-site use of internet and school computing facilities for personal financial gain, or damaging the reputation of the school through use of social media must be reported to the Headteacher, or, in the case of misuse by the Headteacher, to the Chair of Governors. If a child protection or radicalisation issue is suspected, a report should also be made to the Designated Safeguarding Lead.

ONLINE LEARNING PLATFORMS

At Moor First, we use SeeSaw to record and store all observations and assessments relating to each child. This is a safe and secure system and enables parents and carers to access their child's learning journey at any time. Parents/carers can share them with their child, family and friends at home. They may use it for home learning tasks/remote learning and post any comments/photographs/recordings of their own. This helps to create a fully holistic view of the child and strengthen the parent partnership.

Safety and security

Staff use iPads/tablets to take the photographs for observations which are be uploaded to the journals. Staff member have a secure login, which is password and pin protected. The iPads/tablets are kept in a secure facility at school and may only be taken home by staff members for specific reasons and with the express consent of management. Staff should have minimal need to work on journals at home but if they wish to do so, they may access the platforms using their own device. Staff are not permitted to download any photographs of the children onto their own devices. If staff do work on the platforms at home they should be aware of any other people around them and make sure they are not overlooked. They must logout as soon as they have stopped working. If any member of staff suspects that their login details have been compromised in any way, they must inform the school safeguarding lead and new login details will be created. All data held on these platforms, are bound by the Data Protection Act. Photographs stored on the iPads/tablets are deleted on a regular basis by a member of staff.

Parents/carers logging in to the platforms can only access their own child's Learning. Parents may input new observations, video recordings, completed work and photo's, and add comments to existing observations/work. They do not have the necessary permission to edit existing content. Regarding the platforms, parents/carers are asked to give permission for:

- Their pupil's name to be used

- Classwork and homework to be uploaded to their personal child's journal/journey
- Photos and videos of their child working to be uploaded to their personal child's journal/journey
- Photos and videos of their child's work and their child working to be shared publically with the class and their families.
- Examples of completed work to be shared on social media sites – X (formerly Twitter)/facebook.

If parents withhold consent for any of these, class teachers are informed so that they can ensure GDPR compliance when using these platforms.

The child's information and their Learning Journey will be archived from year to year but permanently deleted from our account, once the child leaves our school. Parents will be given the opportunity to download their work at the end of each academic year and if leaving to a new setting**.** Parents without internet: we will print all the information from the platforms and collate it into a paper Learning Journey to support our families.

STAFF GUIDELINES

Staff are advised to use their school email address only for professional use and avoid using it for personal use in order to avoid concerns or accusations of misuse of school computing facilities. Other important documents can be password protected through the email system.

Staff must **never** allow others to use their accounts and should not reveal their password to others. The Headteacher must be informed if it is suspected that someone else knows your account details or passwords – this information is shared with the DPO (Data protection officer) at School.

Staff must always log off or lock their computer when they finish working. Please do not leave a computer unattended while you are logged on.

Staff must always implement suitable security measures on portable devices such as a PIN or password.

The school network, especially SIMS, allows office staff/management to have access to confidential information about pupils and staff. Staff must ensure that such information remains confidential at all times. The General Data Protection Regulations apply to the school, pupil and staff data. These requirements must be followed. Any queries regarding the requirements and implications of the GDPR must be directed to the School office.

Staff must not use school computing facilities to access inappropriate internet content, for personal financial gain and must only access social networking sites for the purposes of enhancing the teaching and learning experience for pupils.

Staff must be aware of and comply with copyright and ownership restrictions when they copy, download or use in lessons any materials from the internet.

Staff must not send photographs, video or audio of pupils as email attachments nor post photographs, video or audio of pupils on websites unless they have permission to do this from pupils' parents or carers and the permission of the Schools Leadership Team. No pupil should be identifiable by name. All materials must represent the school in an appropriate way.

Staff must not send data relating to pupils or any other restricted data to personal email accounts.
When printing confidential material staff must use a secure print method by using a password protected retrieval system. Any confidential material not retrieved by the owner should be put immediately in confidential waste/shredded.

Staff should be aware that email traffic is retained on school servers even if they are deleted from individual accounts.

Staff must obtain permission from Senior Leaders to use any chat room services. Live chat rooms must not be used unless posts are filtered prior to posting.

Staff must ensure that they adhere to all relevant policies and procedures including, but not limited to GDPR Policy/Data retention policy, safeguarding and professional standards. This list is not exhaustive.

Staff are reminded that misuse of the schools computing facilities, internet or social media to access inappropriate materials or for personal financial gain, or damaging the school's reputation in any way, could result in disciplinary action being taken, including loss of access to computing facilities, a verbal or written warning, suspension or dismissal according to school policy. Extreme cases of misuse and all illegal activity will be reported to the police authorities.

Staff have a duty to report all suspected misuse to the DSL/DDSL or chair of governors.

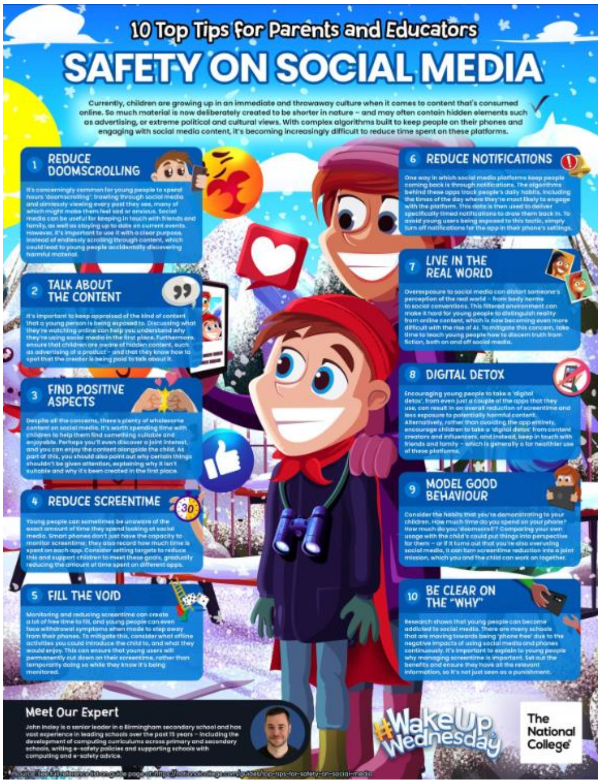
Staff must not leave portable devices such as tablets or mobile phones unattended. Staff must not use software, systems or devices that circumnavigate school managed internet safeguards including the use of mobile hot spots.

TRAINING

All staff attend regular training sessions to ensure they are up to date with all e-safety regulations and to remain compliant with GDPR regulations. During these sessions, governors are invited to attend and the link governor attends. All staff and governors compete annual cyber security training which is recorded by the secretary and monitored by Headteacher. All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. Staff are updated through weekly briefing notes and email bulletins.

PARENTAL SUPPORT

Pupils could potentially have unsupervised internet or social media access at home or at other locations away from the school. All parents or carers should be aware of the concerns and benefits of internet and social media use. Parents and carers are invited to contact the school at any time for advice on safe use of the internet and social media. The school will also provide regular information for parents and carers, for example, through talks on internet safety, the safe use of the internet and social networking sites. As a school we promote safer internet practice through Wake Up Wednesday posters on our social Media:



10 Top Tips for Parents and Educators

SAFETY ON SOCIAL MEDIA

Currently, children are growing up in an immediate and throwaway culture when it comes to content that's consumed online. So much material is now deliberately created to be shorter in nature – and may often contain hidden elements such as advertising, or extreme political and cultural views. With complex algorithms built to keep people on their phones and engaging with social media content, it's becoming increasingly difficult to reduce time spent on these platforms.

1 REDUCE DOOMSCROLLING

It's concerningly common for young people to spend hours 'doomscrolling': trawling through social media and aimlessly viewing every post they see, many of which might make them feel sad or anxious. Social media can be useful for keeping in touch with friends and family, as well as staying up to date on current events. However, it's important to use it with a clear purpose, instead of endlessly scrolling through content, which could lead to young people accidentally discovering harmful material.

2 TALK ABOUT THE CONTENT

It's important to keep appraised of the kind of content that a young person is being exposed to. Discussing what they're watching online can help you understand why they're using social media in the first place. Furthermore, ensure that children are aware of hidden content, such as advertising of a product – and that they know how to spot that the creator is being paid to talk about it.

3 FIND POSITIVE ASPECTS

Despite all the concerns, there's plenty of wholesome content on social media. It's worth spending time with children to help them find something suitable and enjoyable. Perhaps you'll even discover a joint interest, and you can enjoy the content alongside the child. As part of this, you should also point out why certain things shouldn't be given attention, explaining why it isn't suitable and why it's been created in the first place.

4 REDUCE SCREENTIME

Young people can sometimes be unaware of the exact amount of time they spend looking at social media. Smart phones don't just have the capacity to monitor screentime; they also record how much time is spent on each app. Consider setting targets to reduce this and support children to meet these goals, gradually reducing the amount of time spent on different apps.

5 FILL THE VOID

Monitoring and reducing screentime can create a lot of free time to fill, and young people can even face withdrawal symptoms when made to step away from their phones. To mitigate this, consider what offline activities you could introduce the child to, and what they would enjoy. This can ensure that young users will permanently cut down on their screentime, rather than temporarily doing so while they know it's being monitored.

6 REDUCE NOTIFICATIONS

One way in which social media platforms keep people coming back is through notifications. The algorithms behind these apps track people's daily habits, including the times of the day where they're most likely to engage with the platform. This data is then used to deliver specifically timed notifications to draw them back in. To avoid young users being exposed to this tactic, simply turn off notifications for the app in their phone's settings.

7 LIVE IN THE REAL WORLD

Overexposure to social media can distort someone's perception of the real world – from body norms to social conventions. This filtered environment can make it hard for young people to distinguish reality from online content, which is now becoming even more difficult with the rise of AI. To mitigate this concern, take time to teach young people how to discern truth from fiction, both on and off social media.

8 DIGITAL DETOX

Encouraging young people to take a 'digital detox', from even just a couple of the apps that they use, can result in an overall reduction of screentime and less exposure to potentially harmful content. Alternatively, rather than avoiding the app entirely, encourage children to take a 'digital detox' from content creators and influencers, and instead, keep in touch with friends and family – which is generally a far healthier use of these platforms.

9 MODEL GOOD BEHAVIOUR

Consider the habits that you're demonstrating to your children. How much time do you spend on your phone? How much do you 'doomscroll'? Comparing your own usage with the child's could put things into perspective for them – or if it turns out that you're also overusing social media, it can turn screentime reduction into a joint mission, which you and the child can work on together.

10 BE CLEAR ON THE "WHY"

Research shows that young people can become addicted to social media. There are many schools that are moving towards being 'phone free' due to the negative impacts of using social media and phones continuously. It's important to explain to young people why managing screentime is important. Set out the benefits and ensure they have all the relevant information, so it's not just seen as a punishment.

Meet Our Expert

John Insley is a senior leader in a Birmingham secondary school and has vast experience in leading schools over the past 15 years – including the development of computing curriculums across primary and secondary schools, writing e-safety policies and supporting schools with computing and e-safety advice.

Source: See full reference list on guide page at: https://nationalcollege.com/guides/top-tips-for-safety-on-social-media

USAGE RULES AND GUIDELINES

Privacy

The school will access pupil and staff accounts and may review documents and log files in order to ensure that inappropriate use is not taking place. School equipment such as laptops, tablets or mobile phones may be checked from time to time and will be checked on return to ensure that it has been used appropriately.

Software

Pupils and staff must not download, load or install software, shareware or freeware, nor load any such software from USB pens or other memory storage devices without first consulting and obtaining permission from the Network Manager. All software installed must have an appropriate, current licence which must be provided to the Office Staff / Computing Curriculum Leader.

Sharing Files

Pupils and staff must not copy each other's work or intrude into each other's files without permission. Please be aware of compliance with copyright when copying or downloading any materials from the internet, portable media or memory storage devices.

Back up

The school network is backed up by the LA. However, pupils and staff are also encouraged to make back up files for their work via encrypted hard drive and for work not held on the school network. We are working towards a Cloud based facility. Pupils and staff using personal portable devices such as tablets or mobile phones should ensure suitable backup solutions are implemented and maintained.

Purchasing Hardware and Software

The Network Manager must always be consulted before any hardware or software is purchased to ensure that it is compatible with the school network and GDPR compliant. Failure to do so may prevent this hardware or software from being installed on the network.

Cyber Security and Device Protection

The school network is protected against malicious attack or use by various systems such as anti-virus software and firewalls. It is the responsibility of pupils and staff to ensure that any personal computing equipment is also similarly protected against malicious attack or use. It is also preferable that any portable media such as USB pens or DVD's are also scanned for malicious software before they are used on schools equipment. Care should also be taken when opening emails or attachments; always first contact the IT Curriculum Leader / Office Staff or DPO before opening any suspicious or dubious email or attachment.

Inappropriate Materials or Language, Chat Rooms and Computer Games

Abusive materials or language should not be used to communicate nor should such materials be accessed. A good rule is never to view, send or access materials, which you would not want governors, pupils, staff or parents to see. If encountered, such materials should be immediately reported in accordance with this policy. Live chat rooms must not be used unless posts are filtered prior to posting.

Pupils and staff should not access chat rooms from the school site unless such chat rooms have an educational purpose and, in the case of pupils, they have been specifically directed to do so by a teacher or other supervising adult.

It is not appropriate for staff and pupils to play computer or internet games during the school day unless they have an educational purpose or at social times and, in the case of pupils, they have been directed to do so by a teacher or other supervising adult.

All teachers and parents should ensure that video looping is turned off on YouTube, and when children are filming. Children need to know the dangers of filming on the internet at home.

Theft, Vandalism and Wilful Damage to Computing Facilities

Theft and vandalism deplete the school's resources and are detrimental to the learning of pupils. Pupils are expected to treat all computing facilities with respect. Staff should ensure that pupils are supervised when using computing facilities and that any incidents of theft or vandalism are challenged, recorded and dealt with in an appropriate manner. It is important that computing facilities remain secure at all times. Rooms and areas containing computing facilities, for example, must not be left unlocked and unsupervised during open days, parents' evenings and other events when members of the public could be on site unsupervised.

Consequences for Misuse by Pupils

- Access to the wireless network will be removed.
- Device taken away for the period.
- Pupil is not allowed to use personal devices at school.
- Serious misuse of Internet capable devices is regarded as a serious offence and will be dealt with in accordance with this policy.

PUPIL MONITORING

Monitoring of pupil activity will be undertaken routinely as part of the school Safeguarding procedures. The authorised personnel are:

- Headteacher / Designated Safeguarding Lead
- Deputy Designated Safeguarding Lead
- Computing Lead
- IT technician
- Teachers
- Teaching assistants

STAFF MONITORING

Monitoring of staff activity must be authorised by the Headteacher. Monitoring will be at the request of the Headteacher where there is reason to believe the individual has acted inappropriately or contrary to their contract of employment. Monitoring reports will be accessed on 'Securus' by the headteacher.

LINKS TO OTHER POLICIES AND DOCUMENTS

Pupils and staff are reminded that the guidelines and expectations for good conduct in and around the school that are set out in the following policies and apply to use of the schools computing facilities, the internet and social media:

- Behaviour for learning / Anti Bullying.
- Safeguarding
- Pupil / Staff/ Governor Acceptable Use Agreements
- Teacher Professional Standards
- GDPR Policy
- Data Retention

. Code of Conduct for Staff
. Staff Handbook