






Walmsley C of E School

Online Safety Policy

Date Drafted	October 2020
Policy Written By	Miss K Worsley
Date Reported to Governors	September 2021
Date Reviewed	September 2022
Date of Next Review	September 2023
Responsible Committee	School Effectiveness

Mission Statement

As a school we pledge to:

-  Be a happy school where pupils are encouraged and challenged to reach their full academic and social potential in a creative, friendly and safe Christian environment.
-  Work as a partnership with pupils, their families, staff and the wider community to provide an environment of honesty, responsibility and integrity.
-  Give ownership of the opportunities presented to the school family, thus enabling them to reflect on their time at Walmsley with pride.

Statement of Intent

Walmsley CE School believes that Online Safety is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. Internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online.

We have a duty to provide the school community with quality internet access to raise education standards, promote achievement, support professional work of staff and enhance management functions.



Appendices

Appendix	
1	Online Safety Incident Flowchart
2	School Technical Security Overview
3	AUP documents – Staff / Pupils / Visitors <ul style="list-style-type: none"> - EYFS/KS1 AUP - Y3/4 AUP - Y5/6 AUP - Staff, Governor and Volunteer AUP
4	School Data Protection <ul style="list-style-type: none"> - Parent / Carer Privacy Notice - Child Friendly GDPR Document - Workforce Privacy Notice

Scope of the Policy

The regulation and use of technical solutions to safeguard children are important but must be balanced with teaching the necessary skills to enable pupils to take responsibility for their own safety in an ever changing digital world. The National Computing Curriculum states that children should be able to use technology safely, respectfully, and responsibly keeping personal information private, recognise acceptable or unacceptable behaviour and identify a range of ways to report concerns about content and contact. Children's safety is paramount and they will receive the help, guidance and support through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum staff will reinforce and consolidate safe online learning.

This policy applies to all members of the school community who have access to and are users of school ICT systems and online resources, both in and out of school.

The school will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and anti-bullying policies (and others when applicable).

Development of the Policy

This Online Safety Policy has been developed by a working party led by Bolton Schools' ICT. It is recommended that this Policy is reviewed and ratified by the school's own relevant parties* i.e.

- Headteacher: Mrs J Atherton
- Governing Body: Mr R Dyson
- Safeguarding Lead: Mrs J Atherton
- Computing Lead: Miss K Worsley

Schedule of Monitoring and Review

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new Online threats or incidents that have taken place.

The implementation of this Online Safety Policy will be monitored by the:

- Headteacher: Mrs J Atherton
- Governing Body: Mr R Dyson
- Safeguarding Lead: Mrs J Atherton
- Computing Lead: Miss K Worsley

The school will monitor the impact of the policy using:

Logs of reported incidents.
Monitoring logs of internet activity (including sites visited).
Internal monitoring data for network activity.

Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Where appropriate
Should serious online incidents take place, the following external persons / agencies should be informed:	Headteacher School Safeguarding Lead LADO Police See Appendix 1

Roles and Responsibilities

Headteacher:

The Headteacher has a duty of care for ensuring the day to day safety (including online) of all members of the school community.

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meeting at regular intervals with the Computing Lead to ensure the implementation of this policy (as outlined above). It is recommended that regular subject leader time is allocated to fulfil the role
- ensuring the relevant parties receive regular monitoring reports from the Computing lead
- ensuring there are opportunities to communicate up to date online safety information to the wider school community.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

Governors:

Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing board, receiving regular information about online incidents and monitoring reports.

The role of the Online Governor will include:

- regular meetings with the Computing Lead/Team
- regular monitoring of CPOMS which will include anonymous details of Online Incidents
- ensuring robust technical support is in place to keep systems safe and secure
- regular monitoring of filtering
- reporting to the Governing board
- attending training for online safety where appropriate.

Safeguarding Lead

The Safeguarding Lead is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (**Appendix 1**).

** If a school is using CPOMS, it is important to ensure that the lozenges are set up to be specific and appropriate, for example – PEGI, SnapChat, Instagram, etc. This will assist in collating and responding to online incidents.

They will be trained in online issues and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to:

- sharing of personal data
- accessing illegal / inappropriate materials
- exposure to inappropriate online content
- inappropriate contact with adults/strangers
- potential or actual incidents of grooming
- sexting
- cyber-bullying

In the event of a child protection or safeguarding incident pertaining to the above, the safeguarding lead will refer to Appendix 1.

Computing Lead / Team

The Computing Lead / Team is responsible for the management of online issues and take a leading role in establishing and reviewing the school Online Safety Policy.

The role of the Computing Lead/team includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant outside agencies
- liaising with relevant technical support teams
- collating and reviewing reports of Online Incidents on **CPOMS**)
- meeting regularly with Headteacher and relevant parties to discuss issues and subsequent actions
- taking action in response to issues identified
- communicating up-to-date Online Safety information to the wider school community.

School Staff

It is essential that all staff

- understand and acknowledge their responsibilities as outlined in this Policy
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD
- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents CPOMS
- when addressing any suspected misuse or Online Safety Issue, refer to Appendix 1
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems
- apply this Online Safety Policy to all aspects of the Curriculum
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate Acceptable Use Policy
- are good role models in their use of all digital technologies
- are vigilant in monitoring how pupils use digital technologies and access online content whilst in their care.

It is accepted that from time to time, for purposeful/appropriate educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable with clear reasons for the need.

Technical Support

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack.

To facilitate this, school has support from Bolton Schools ICT: Mr M Whittle

The role includes:

- ensuring that detected risks and/or misuse is reported to the Headteacher at school
- ensuring that schools are informed of any changes to guidance or any planned maintenance
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements
- all users will have clearly defined access rights to school technical systems and devices
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list
- content lists are regularly updated and internet use is logged and regularly monitored
- there is a clear process in place to deal with requests for filtering changes
- provide a platform where school should report any content accessible in school but deemed inappropriate
- ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software (**Appendix 2**)

Pupils

The children's learning will progress through a broad, effective and relevant Online Safety curriculum.

A pupils learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing.

It is essential that all pupils should:

- understand, acknowledge and adhere to their age-appropriate Acceptable Use Policy (**Appendix 3**)
- be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it
- accept their responsibility to respond accordingly to any content they consider as inappropriate
- understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school
- know that school will take action in response to any breach of the Online Safety Policy

Parents / Carers / Responsible adults

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line usage. Due to the ever evolving Digital World, adults can sometimes be unsure of how to respond to online risks and issues. They may also underestimate how often pupils encounter potentially harmful and inappropriate online material.

Therefore, it is essential that all adults should:

- promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events
- understand, acknowledge and adhere to their child's Acceptable Use Policy (**Appendix 3**)
- understand, acknowledge and ensure that their child adheres to school procedure relating to their use of personal devices whilst on school grounds

To support the school community, school will provide information and awareness through, but not limited to:

- letters, newsletters, website links, publications, external agencies
- Parents / Carer workshops
- high profile events / campaigns e.g. Safer Internet Day

Visitors Entering School

It is essential that school apprise visitors of all relevant policies pertaining to their visit and contact with pupils.

Useful Information

Safeguarding

In the event of a Safeguarding infringement or suspicion, appendix 1 must be followed with consideration of the following:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported
- Conduct the procedure using a computer that will not be used by pupils and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record 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 and signed (except in the case of images of child sexual abuse – see below)

- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the relevant group for evidence and reference purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy (**Appendix 4**).

Communications

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

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.
- When accessing emails out of the schools setting, staff will only be able to access their schools emails using Microsoft Multifactor Authentication app.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media

The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils.

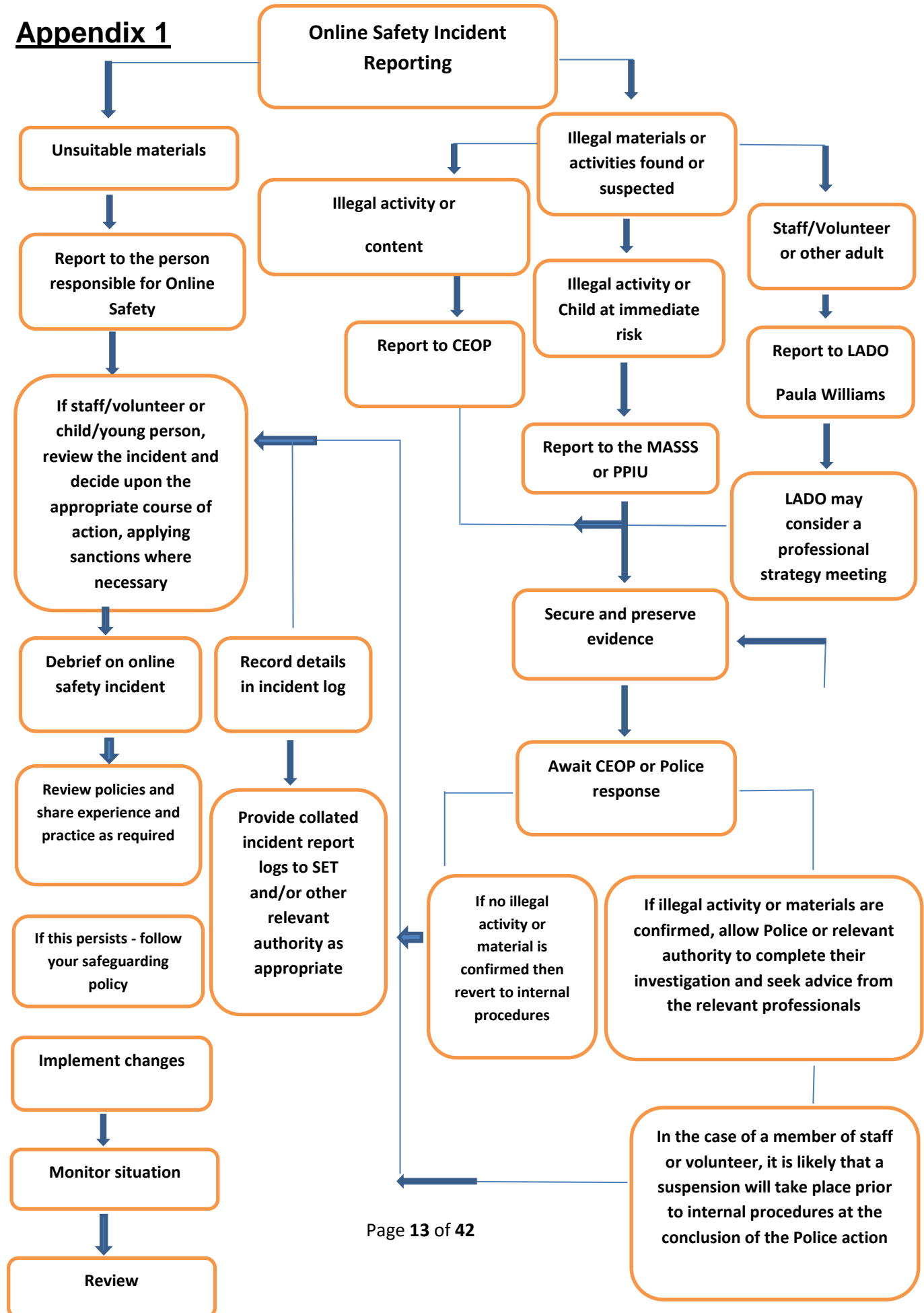
Use of personal mobile phones to take photos/videos of Walmsley CE School children

At Walmsley, we have an active twitter account and website where we post many photos of the children at our school. All permanent teaching staff are issued a school mini iPad and are encouraged to use these to take photos/videos to upload onto our school Twitter account, blog or website.

We also allow staff to take photos of the children on their own personal mobile phones/devices, however staff must delete these photos/videos as soon as they have been tweeted/posted. (Tweet it, delete it).

If staff do wish to use their **personal** mobile phone/device in this manner they must sign the agreement (Staff, Governor, Visitor AUP) which allows the head teacher to have the right to check the photo or video content of their phone if she felt the need to. If staff, do not wish to sign this agreement, then all photographs and videos taken of children from school must be done so on school equipment only (school mini-iPad, school cameras or school iPad) and not on their **personal** devices (mobile phone, iPad, laptop etc).

Appendix 1



Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

LADO: Paula Williams - 01204 337474

Bolton's MASSS – 01204 331500

Police Protection Investigation Unit – 0161 856 7949

Community Police – 101

EXIT Team – 01204 337195

Bolton Safeguarding Children's Board: Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or

contact@sict.bolton.gov.uk

Appendix 2: School Technical Security Overview

ICT Guidance for OfSTED Inspection

It has been brought to our attention that during recent OfSTED inspections, questions have been asked about procedures schools are using for internet filtering and security.

We produced the notes below to assist one colleague with this and the information seemed to be helpful when answering the inspector's questions.

Therefore, I am sharing this to hopefully be of assistance should your school be inspected.

Should you need any further assistance during inspection regarding ICT issues, please contact the unit and we will assist wherever possible.

For Bolton schools subscribing to Bolton Schools ICT (Bolton SICT) Broadband services, internet access is via the local authority maintained Wide Area Network.

We use a central internet filtering system for all schools.

This is an industry standard solution, Sophos Universal Threat Management, the product incorporates the IWF standards.

We have this configured as per DFE guidelines, see following technical blog post:
<https://technical.bolton365.net/internet-filtering/>

The system can also be deployed at school level if required, but the standard configuration has distinct filtering levels for staff and pupils.

Filtering change requests are online and are only accepted from authorised users. Any changes are security checked before implementation.

The system provides Bolton SICT with full monitoring and reporting, these reports are available to schools when requested.

Bolton Schools ICT Broadband service also includes:

- *Email content filtering*
- *Email anti spam*
- *Secure email facilities – Multi Factor Authentication*
- *Full anti virus*
- *Encrypted document exchange*
- *2 factor remote access*
- *Industry standard firewalls to protect both WAN and school LANs*

Bolton School ICT staff that maintain these systems are all minimum Microsoft qualified and have many years industry experience.

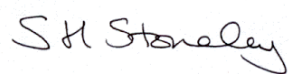
The Inspectors have also indicated that pupils from Year 1 onwards should be using individual logins to allow monitoring of computer usage.

Some schools are already doing this, from EYFS, for network, Purple Mash and blog logon, using a four digit password.

If your school requires this facility, please contact the unit via email at contact@sict.bolton.gov.uk

For devices, such as iPads, that do not use network logins, we are currently looking at ways of user authentication to provide monitoring.

Yours sincerely

A handwritten signature in black ink that reads "S H Stoneley". The signature is written in a cursive style with a large 'S' and 'H'.

Sam Stoneley

Schools ICT Unit Manager

Tel: 01204 332034

Fax: 01204 332235





Email: Sam.Stoneley@sict.bolton.gov.uk

Appendix 3: AUP documents – Staff / Pupils / Visitors

- EYFS/KS1 AUP
- Y3/4 AUP
- Y5/6 AUP
- Staff, Governor and Volunteer AUP

Appendix 3

EYFS and Key Stage 1 Acceptable Use Policy

 My Learning	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.
 My Online Safety	<ul style="list-style-type: none"> • I will always use what I have learned about Online Safety to keep myself safe. • I will tell a teacher if I see something that upsets me on the screen.
 Using the Internet @school	<ul style="list-style-type: none"> • I will only use the internet when the teacher says I can. • I will only go on websites that my teacher allows me to. • I will tell my teacher if I go on a website by mistake.
 Using the Internet @home	<ul style="list-style-type: none"> • I will tell a trusted adult if I see something that upsets me on the screen.

I understand that these rules help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

Child's Signature: _____

Parents / Carers:

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.




I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent / Carer Signature: _____ **Date:** _____

Appendix 3

Year 3 and Year 4 Pupils School Acceptable Use Policy

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ iPads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> • I will only visit sites that are appropriate to my learning at the time <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may use it. <p>My role as a Digital Citizen.</p> <ul style="list-style-type: none"> • I will report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> • I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies eg: CEOP, Childnet, Childline, Barnardos <p>My Communications</p> <ul style="list-style-type: none"> • I will be aware of the "SMART" rules, when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use inappropriate language and I understand that others may have different opinions. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

Child's Signature

Parents / Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.




I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent / Carer Signature: _____ **Date:** _____

Appendix 3

Year 5 and Year 6 Pupils Acceptable Use Policy

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will use school devices (PCs, laptops, tablets/ ipads) for my learning. • I will ask a teacher before using a device and ask for help if I can't work the device. • I will only use activities that a teacher has told or allowed me to use. • I will ask a teacher if I am not sure what to do or I think I have done something wrong. • I will look after the school's computing equipment and tell a teacher if something is broken or not working properly. • When logging on using my own username and password, I will keep it safe and secret. • I will save only school work on the school computer and will check with my teacher before printing. • I will log off or shut down a computer when I have finished using it.
 <p>Using the Internet @school</p>	<ul style="list-style-type: none"> • I will only visit sites that are appropriate to my learning at the time <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my username and password safe and secure - I will not share it. • I will not try to use any other person's username and password. • I understand that I should not write down or store a password where it is possible that someone may steal it. <p>My role as a Digital Citizen.</p> <ul style="list-style-type: none"> • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images of anyone without their permission.
 <p>Using the Internet @home</p>	<ul style="list-style-type: none"> • I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, school details) • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line, to a trusted adult or online agencies e.g.: CEOP, Childnet, Childline, Barnardos. <p>My Communications (Including texting and messaging)</p> <ul style="list-style-type: none"> • I will be aware of "stranger danger", when I am communicating online. • I will be polite and responsible when I communicate with others. • I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions. <p>My use of Social Media and Gaming</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying.

I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

I understand that these rules, help me to stay safe and I agree to follow them.
I also understand that if I break the rules I might not be allowed to use school computing equipment.

My parents/carers understand that keeping me safe on the internet at home is their responsibility.

Child's Signature

Parents / Carers:

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Parent/Carer's Signature

Date

Appendix3:

Staff, Governor and Volunteer Acceptable Use Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- That staff, governor and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, governors and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff, governors and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my professional and personal safety:

- I understand that Walmsley CE School will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

Staff passwords:

- **All staff users will be provided with a username and initial password by Bolton Schools ICT who will keep an up to date record of users and their usernames.**

- **Initial passwords will be changed on first use, and only then be known to that user**
- *the password should be a minimum of 7 characters long and must include three of – uppercase character, lowercase character, number, special characters, must not include proper names or any other personal information about the user that might be known by others*
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the appropriate person
- I will be professional in my communications and actions when using *school* ICT systems:
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website /blog) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with pupils / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. Staff are not to use personal email addresses for communication. Personal mobile devices can be used for taking photographs for Twitter and Tapestry, but must be deleted straight away. "Post it, delete it!"
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (laptops / iPads / mobile phones) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by Walmsley CE School about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, without permission.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Policy.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

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

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- **I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action.**

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

Staff / Volunteer Name

Signed

Date

Appendix 4

Parent / Carer Privacy Notice

Policy Statement

We are Walmsley CE Primary School. During your child's time with us, we will gather and use information relating to you. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from you directly and data about you that we obtain from other people and organisations. We might also need to continue to hold your personal data for a period of time after your child has left the School. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about you, why we process that data, who we share this information with, and your rights in relation to your personal data processed by us.

What information do we process in relation to you?

We will collect, hold, share and otherwise use the following information about you:

- Personal information (such as name, address, home and mobile numbers, personal email address, emergency contact details and relationship marital status)
- Financial details (such as bank account or credit card details), and other financial details such as eligibility for free school meals or other financial assistance
- CCTV footage and images obtained when you attend the School site
- Your relationship to your child, including any Court orders that may be in place
- Characteristics (such as ethnicity, language, religion, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Relevant medical information and dietary needs
- Special Educational Needs information
- Exclusions & Behavioural information
- Child Protection and Safeguarding information

We will also use special categories of data such as gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, information about health, genetic information and biometric data. These types of personal data are subject to additional requirements.

Where do we get your personal data from?

We will obtain an amount of your personal data from you, by way of information gathering exercises at appropriate times such as when your child joins the School, and when you attend the School site and are captured by our CCTV system.

We may also obtain information about you from other sources. This might include information from the local authorities or other professionals or bodies, including a Court, which might raise concerns in relation to your child.

Why do we use your personal data?

We will process your personal data for the following reasons:

1. Where we are required by law, including:
 - To provide reports and other information required by law in relation to the performance of your child
 - To raise or address any concerns about safeguarding
 - To the Government agencies including the police
 - To obtain relevant funding for the school
 - To provide or obtain additional services including advice and/or support for your family
 - To support pupil learning
 - To provide appropriate pastoral care
 - To assess the quality of our services
 - To comply with the law regarding data sharing
 - To enable us to provide a responsible and safe school for the benefit of our children in a particular geographical area
 - To monitor and report on pupil assessments, progress and records
 - To manage our staff, pupils, governors, employees and volunteers
 - To maintain our own accounts and records
 - To inform you of news, events, activities and services running at Walmsley CE Primary School
 - To share your contact details with the DFE and Local Authority so they can keep you informed on statistical research activities and in which you may be interested
 - Where the law otherwise allows us to process the personal data as part of our functions as a Primary School, or we are carrying out a task in the public interest, including:
 - To confirm your identity
 - To communicate matters relating to Walmsley School to you
 - To safeguard you, our pupils and other individuals
 - To enable payments to be made by you to Walmsley School
 - To ensure the safety of individuals on Walmsley School site
 - To aid in the prevention and detection of crime on Walmsley School site
2. Where we otherwise have your consent

Whilst the majority of processing of personal data we hold about you will not require your consent, we will inform you if your consent is required and seek that consent before any processing takes place.

Why do we use special category personal data?

We may process special category personal data in relation to you for the following reasons:

1. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Data Protection Policy.

[There is a specific requirement in the Data Protection Bill for an appropriate policy document to be in place in relation to processing of special category personal data for employment law purposes.]

2. Where the processing is necessary in order to ensure your health and safety on the Walmsley School site, including making reasonable adjustments for any disabilities you may have.
3. Where we otherwise have your explicit written consent.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests of those of your child, and where it is not possible to seek your consent.

Failure to provide this information

If you fail to provide information to us, we may be prevented from complying with our legal obligations.

How long will we hold your personal data for?

We will hold your personal data only for as long as necessary. How long we need to hold on to any information will depend on the type of information. For further detail, please see our Information Management Policy.

Who will we share your personal data with?

We routinely share information about you with:

- Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education [and/or the Education and Skills Funding Agency], in compliance with legal obligations of the school to provide information about students and parents as part of statutory data collections
- Contractors, such as payment processing providers to enable payments to be made by you to the Walmsley School
- Schools that the pupil's attend after leaving us
- The school nurse / NHS / Health and other professionals working with specific pupils
- Early Intervention Team
- Emergency contact telephone numbers are accessed by Eduspot (Teachers2Parents Texting Service and Parents Evening Booking System).
- Child's name only for trips recorded on Tucasi accounting package
- SBS online, accounting software, staff data only
- Times Table Rockstars - child's name and cohort

- Tapestry – online learning journal – child’s learning journey, parents/carers email addresses
- Christ Church Walmsley, to assist in the Journey of Faith i.e. Confirmation.

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department’s data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>.

Contact details for the Department can be found at <https://www.gov.uk/contact-dfe>.

Local authorities may share information that we are required to provide to them with other organisations. For further information about Bolton Local Authority’s data sharing process, please visit: <https://www.bolton.gov.uk>

Contact details for Bolton Local Authority are:

Information Management Unit
Department of People
Bolton Council
1st Floor
Town Hall
Bolton
BL1 1UA

Your rights in relation to your personal data held by us

You have the right to request access to personal data that we hold about you, subject to a number of exceptions. To make a request for access to your personal data, you should contact:

Mrs J Atherton
Headteacher
Walmsley CE School
Blackburn Road
Egerton
Bolton
BL7 9SA

Please also refer to our Information Management Policy for further details on making requests for access to your personal data.

You also have the right, in certain circumstances, to:

- Object to the processing of your personal data
- Have inaccurate or incomplete personal data about you rectified
- Restrict processing of your personal data
- Object to the making of decisions about you taken by automated means

- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of your data protection rights

If you want to exercise any of these rights then you should contact the Headteacher using the above contact details. The law does not oblige the school to comply with all requests. If the school does not intend to comply with the request then you will be notified of the reasons why in writing.

Concerns

If you have any concerns about how we are using your personal data then we ask that you contact our Data Protection Officer in the first instance. However an individual can contact the Information Commissioner's Office should you consider this to be necessary, at the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at:

The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Contact


If you would like to discuss anything in this privacy notice, please contact:

Mrs K Wilkinson
Harwood Data
6 Everleigh Close
Harwood
Bolton
BL2 3HE

Appendix 4

Walmsley CE Primary School Pupil Privacy Notice

What's this about?

 A new law is being made that keeps your information safe – things like your address, date of birth and phone number. The school and other people collect and use information for all kinds of reasons, and the new law tells them exactly what they are allowed to do with yours.

We collect some information about our pupils, like you. It's our job to tell you how we will collect the information, how we will record it and how we will use it.

In this notice, you will see different names or terms used that you may not be familiar with, such as:

Data controller: This person (or group of people, like a school) is in charge of the information we collect.

Data processor: This person processes information for the data controller.

Data protection officer (DPO): This person makes sure we do everything the law says. The school's DPO is Mrs J Atherton, Headteacher.

Personal data: This means any information that can be used to identify someone, such as your address and date of birth.



Who looks after your information?

The school is the data controller of the personal information you give us – we look at how and why your information is collected and used.

Sometimes the school has to give your information to other people, such as the government, but it will only give away your information when you say it's ok or when the law says that they have to. When your data is given to someone else, they must look after it and keep it safe.

Why do we collect and use your information?

We will only collect your information when we need it to help us do our job or to follow the law. When we've collected it, here's how we use it:

- **To support your learning**
- **To monitor and report on your progress**
- **To provide appropriate support**
- **To assess the quality of our service**
- **To comply with the law regarding data sharing**



What information do we collect?

The categories of information that the school collects, holds and shares include the following:

Your personal information

This is things like your name and address.

Your characteristics

This means information about you, like where you're from, what language you speak and things like that.

Your attendance information

We will also record how many times you missed school and why you couldn't come to school.

Your assessment information

We collect your test results when you sit a big test or exam.

Some of your medical information

We keep information about any times you've been ill and any special conditions you have that we need to know about to keep you safe.

Any needs you have

We collect information that helps us teach you better, such as any special educational needs, behaviour needs you may have.

Photography

Using photographs of you counts as processing your personal data. Before we take or use any photographs we will ask you (if you're old enough) or a parent to give permission for us to take and use pictures of you. We might use your pictures on display boards or on the school's website, for example.



Do you have to give us your information?

You must give us quite a lot of the information we need, but there is some information that you can choose whether to let us have it or not.

When we ask you for information that you don't have to give us, we will ask for your permission and let you know why we want it and what we will do with it. If you don't want us to have the information, that's your choice.



How long will we keep your information?

We don't keep it forever, only for as long as we need it to help us do the thing we needed it for. We have a policy that tells us when to keep it and when to bin it.



Will your information be shared?

We won't share your information with anyone else without your permission, unless the law says we can or should. We may share information with:

- **The LA**
- **The NHS - school doctor or nurse**
- **The DFE**
- **Courts – if requested**
- **Your next school**

The information that we share with them includes:

- **Your unique pupil number and nationality**
- **Your attendance at school**
- **School meal type**
- **Special Educational Needs**
- **Your next school to enable transition**

Sometimes we have to share your information. We normally have to share it with the people in charge of all schools, the Department for Education (DfE). They may ask us to share things like:

- **Pupils on roll at the school**
- **Attendance figures**
- **Performance data**
- **Our Local Authority**

They store some of their information in the National Pupil Database, and then share some of it with people looking to help schools and pupils like you. But don't worry, the database is very safe and your information won't get lost or given to anyone who shouldn't have it.

Your parents can ask us to only share your name, address and date of birth, and nothing else, by sending an **email or letter** to Mrs A Crowther. When you're 16, it's up to you to decide what information you want to share.

You can find out more online: **LA's website link**.



What are your rights?

You and your parents have the right to:

- Be told how we use your information.
- Ask to see the information we hold.
- Ask us to change information you think is wrong.
- Ask us to remove information when it's not needed anymore.
- Ask us to only use your information in certain ways.
- Tell us you don't want your information to be processed.

If the information we are collecting is information that you can choose not to give, you can tell us to stop collecting it at any time.

If you're worried about how we get and use your information, you can speak to the Headteacher at the school, who will be able to help you and answer any questions that you have. If you want to speak to somebody not at the school, you can call the people who look after information, called the Information Commissioner's Office (ICO), on 0303 123 1113 or using their [live chat](#).



Would you like to know more?

If you or your parents would like to find out more information about how we and/or the DfE collect, use and store your personal information, please visit our website **www.walmsley.bolton.sch.uk**

Four important things to understand

Now you have read this, we hope you understand that:

- The law allows us to get and use your information to help us do our job.
- We may share your information with others, but only when we really need to.
- We will ask for your permission to share your information whenever you have a choice.
- You can tell us not to share your information, even when you have said yes before.

If you have any questions, Mrs Atherton will be happy to help you.

Appendix 4

Workforce Privacy Notice

Policy Statement

We are Walmsley CE Primary School. During an individual's time with us, we will use information that we gather in relation to them for various purposes. Information that we hold in relation to individuals is known as their "personal data". This will include data that we obtain from the individual directly and data about the individual that we obtain from other people and organisations. We might also need to continue to hold an individual's personal data for a period of time after they have left the school. Anything that we do with an individual's personal data is known as "processing".

This document sets out what personal data we will hold about our workforce, why we process that data, who we share this information with, and the rights of individuals in relation to their personal data processed by us.

What information do we process in relation to our workforce?

We will collect, hold, share or otherwise use the following information about our workforce:

- personal information (such as name, address, home and mobile numbers, personal email address, employee or teacher number, national insurance number, and emergency contact details)
- contract information (such as start dates, hours worked, post, roles and salary information, bank/building society details)
- work absence information (such as number of absences and reasons (including information regarding physical and/or mental health), holiday records)
- qualifications / training courses attended and, where relevant, subjects taught (such as training record)
- performance information (such as appraisals and performance reviews, performance measures including performance management/improvement plans, disciplinary or grievance records)
- other information (such as pension arrangements (and all information included in these necessary to administer them), time and attendance records, information in applications made for other posts within the school, criminal records information (including the results of Disclosure and Barring Service (DBS) checks), details in references the school receives or provides to other organisations, CCTV footage and images)

We will also use special categories of data including such as gender, age, ethnic group, sex or sexual orientation, religious or similar beliefs, political opinions, trade union membership, information about health, genetic information and biometric data. These types of personal data are subject to additional requirements.

Where do we get information from about our workforce?

A lot of the information we have about our workforce comes from the individuals themselves. However, we may also obtain information from tax and regulatory authorities such as HMRC, previous employers, your trade union, the DBS, our insurance benefit administrators, consultants and other professionals we may engage, recruitment or vetting agencies, other members of staff, students or their parents, and publically available resources including

online sources. In addition we may obtain information from automated monitoring of our websites and other technical systems such as our computer networks and systems, CCT and access control systems, communications systems, remote access systems, email and instant messaging systems, intranet and internet facilities, telephones, voicemail and mobile phone records.

Why do we use this information?

We will process the personal data of our workforce for the following reasons:

1. Where we are required by law, including:
 - To comply with the law regarding data sharing (see further below)
 - To comply with specific employment law requirements, including our obligations as an employer under employment protection and health and safety legislation, and under statutory codes of practice such as those issued by ACAS
 - To comply with legal requirements in relation to equalities and non-discrimination
2. Where we are required by any contract with our workforce, such as employment contracts, including:
 - To make payments to our workforce, such as salary payments
 - To deduct tax and National Insurance contributions
 - To make a decision about recruitment
 - To check individuals are legally entitled to work in the UK
 - Administering employment contracts
 - Conducting performance reviews
 - Making decisions about salary and compensation
 - Liaising with pension providers
3. Where the law otherwise allows us to process the personal data, or we are carrying out a task in the public interest, including:
 - To enable the development of a comprehensive picture of the workforce and how it is deployed
 - To inform the development of recruitment and retention policies
 - To safeguard our pupils and other individuals
 - To ensure safe working practices
 - In the interests of ensuring equal opportunities and treatment
4. Where we otherwise have the consent of the individual

Whilst the majority of processing of personal data of our workforce will not require consent, we will inform individuals if their consent is required and seek that consent before any processing takes place. Due to the imbalance of power in an employee to employer relationship, it is generally thought that although consent may be implied it cannot truly be freely given. So consent is not necessarily the most appropriate basis to rely upon as an employer.

Why do we use special category personal data?

We may process special category personal data of our workforce for the following reasons:

4. To carry out our legal obligations in relation to employment law, where this is in accordance with our Information Management Policy

[There is a specific requirement in the Data Protection Bill for an appropriate policy document to be in place in relation to processing of special category personal data for employment law purposes. Where the processing is necessary for reasons of substantial public interest, including for purposes of equality of opportunity and treatment, where this is in accordance with our Information Management Policy].

[The same applies as above.]

5. For the purposes of preventative or occupational medicine in order to assess an individual's working capacity and/ or the need for reasonable adjustments.
6. Where we otherwise have an individual's explicit written consent – subject to the restriction set out above on the use of consent in an employment relationship.

There may also be circumstances where we need to use your information in relation to legal claims, or to protect your vital interests and where you are unable to provide your consent.

Failure to provide this information

If our workforce fail to provide information to us then this may result in us being unable to perform the employment contract, or we may be prevented from complying with our legal obligations.

How long will we hold information in relation to our workforce?

We will hold information relating to our workforce only for as long as necessary. How long we need to hold on to any information will depend on the type of information. For further detail, please see our Information Management Policy.

Who will we share information with about our workforce?

We routinely share information about our workforce with:

- Local authorities, to assist them in the exercise of their responsibilities in relation to education and training, youth support and safeguarding purposes
- The Department for Education, in compliance with legal obligations of the school to provide information about our workforce as part of statutory data collections
- Contractors, such as payroll providers, to enable them to provide an effective service to the school and government agencies such as HMRC and DWP regarding tax payments and benefits
- Our professional advisors including legal and HR consultants

The Department for Education may share information that we are required to provide to them with other organisations. For further information about the Department's data sharing process, please visit: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>.

Contact details for the Department can be found at <https://www.gov.uk/contact-dfe>.

Rights of our workforce in relation to their personal data

All of our workforce have the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact:

Mrs J Atherton
Headteacher
Walmsley CE School
Blackburn Rd
Bolton
BL7 9SA

Please also refer to our Information Management Policy for further details on making requests for access to workforce information.

Individuals also have the right, in certain circumstances, to:

- Object to the processing of their personal data
- Have inaccurate or incomplete personal data about them rectified
- Restrict processing of their personal data
- Object to the making of decisions about them taken by automated means
- Have your data transferred to another organisation
- Claim compensation for damage caused by a breach of their data protection rights

If an individual wants to exercise any of these rights then they should contact the Headteacher at the above address. The law does not oblige the school to comply with all requests. If the school does not intend to comply with the request then the individual will be notified of the reasons why in writing.

Concerns

If an individual has any concerns about how we are using their personal data then we ask that they contact our Data Protection Officer in the first instance. However an individual can contact the Information Commissioner's Office should they consider this to be necessary, at <https://ico.org.uk/concerns/>.

Contact

If you would like to discuss anything in this privacy notice, please contact:

Mrs K Wilkinson
Harwood Data
6 Everleigh Close
Harwood
Bolton
BL2 3HE