Data Protection Policy

1. INTRODUCTION

1.1. This Data Protection Policy sets out the roles, responsibilities and procedures around the use of data within SELFA.

1.2. This policy applies whenever you are collecting or handling personal data (as defined in paragraph 3.2) in any way.

1.3. Everyone has rights with regard to the way in which their personal data is handled. In the course of our activities we will collect, store and use personal data about children, parents and guardians, staff, volunteers and people in external organisations.

1.4. This policy applies to all SELFA employees. Any breach of this policy may result in disciplinary action/termination of services by SELFA, as appropriate.

1.5. This policy does not form part of any employee's contract of employment and may be amended at any time.

1.6. Please read this policy alongside our Data Retention Policy.

2. AIMS OF THIS POLICY

2.1. To protect the rights, safety and welfare of individuals, particularly children, in relation to the use of personal data within SELFA.

2.2. To help you understand the fundamentals of data protection law.

2.3. To guide you to help ensure that SELFA is compliant with data protection laws.

2.4. To understand the risks to SELFA of non-compliance with data protection laws.

3. WHAT DOES THE LAW SAY?

3.1. The Data Protection Act (2018) is the UK's implementation of the General Data Protection Regulation (GDPR) and aims to give individuals new rights over their data. These include things such as the right to erasure. We have given a more detailed explanation of these rights below.

What is personal data

3.2. Personal data is any data which relates to a living individual who can be identified from that data (or from that data and other information likely to come into SELFA's possession). It therefore captures a wide range of data. Examples of personal data include names and addresses, bank details, attendance records, incident forms, accident reports and survey responses. If you are unsure about whether certain information is personal data or not, please speak to your Line Manager.

What is special category data

3.3. Special category data is personal data which the GDPR says is more sensitive and so needs special protection. Special category data includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. It is important that you recognise what is special category data because the law imposes more stringent requirements around its use.

Who regulates the GDPR in the UK?

3.4. In the UK, the Data Protection Laws are independently enforced by the Information Commissioner's Office ("ICO").

What happens if we get it wrong?

3.5. The ICO has a wide range of powers. It can issue enforcement notices where it tells business to remedy a certain breach. It can also publicise data protection breaches on its website which could lead to negative publicity for SELFA, if we are in breach. It also has the right to audit SELFA and fine SELFA up to €20 million or 4% of global turnover for breaches of the Data Protection Laws.

The 6 data protection principles

3.6. The GDPR sets out 6 data protection principles which you should be aiming to follow at all times. They are as follows:

(1) Fair, lawful and transparent. The first principle is that personal data shall be processed fairly, lawfully and transparently. The Data Protection Laws are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individuals whose data you are using. It also important to be transparent with individuals in relation to what you do with their data.

(2) Use it only for a limited purpose. The second principle is that personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. As a member of staff at SELFA, you may be involved in collecting personal data in different ways. This may include data you receive directly from individuals (for example, by completing forms) and data you receive from other sources (including, for example, reports from schools or previous employers for employees). You must not use the data for your own personal purposes. Personal data which you collect in the course of your employment, or provision of services, should be used strictly as part of carrying out your role at/for SELFA and only for the purpose for which it was collected.

(3) Data minimisation. The third principle is that personal data shall be adequate, relevant and limited to what is necessary. You should only collect, use, access or analyse personal data to the extent that you need to.

(4) Accuracy. The fourth principle is that personal data shall be accurate and, where necessary, up to date. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You should take all reasonable steps to destroy or amend inaccurate or out-of-date data.

(5) Data retention. The fifth principle is that personal data shall be kept for no longer than is necessary. The Data Protection Laws do not tell us how long is necessary. We have, therefore, prepared a separate Data Protection Retention Policy to guide you in determining how long to keep certain types of information. Please refer to that policy for further details about how long you should be keeping certain types of personal data and how you should be deleting personal data. It is important that you follow the Personal Data Retention Policy and it should be read in conjunction with this policy.

(6) The security principle. The sixth principle is that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful use of personal data and against accidental loss, destruction or damage. The GDPR says that we must use "appropriate, technical and organisational measures" to keep data secure. Security of personal data applies to a range of areas, including IT security, and it should be applied throughout your day-to-day activities. You should review SELFA's IT policies for further details about using IT securely.

3.7. There are additional principles that we believe are just as important as those set out above and these are set out below.

Respecting the individual's legal rights. SELFA will also be required to process personal data in accordance with the rights of data subjects (i.e. the individuals about whom SELFA holds personal data). Please see paragraphs 9 and 10 for further detail about individuals' (particularly parents' and children's) right of access to the information SELFA hold about them (commonly known as a subject access request or "SAR") and their right for information about them to be erased (typically referred to as the right to erasure or right to be forgotten).

Don't let personal data leave the UK without telling us. Personal data must not leave the European Economic Area unless certain legal protections are in place. If you would like further details about this principle or have any queries, please speak to your line manager. If you are aware of personal data being transmitted outside of the UK (for example by using software with servers storing personal data elsewhere) you need to tell your line manager immediately. This might mean having to do some investigation as to how personal data flows in and out of the organisation.

Accountability. We will all need to take responsibility for the principles above and be able to demonstrate that we are complying with them. Please make sure that you are in a position to show your line manager how you are complying with this policy and the Personal Data Retention Policy.

The lawful basis for processing data

3.8. The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data.

(1) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(2) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(3) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(4) Vital interests: the processing is necessary to protect someone's life.

(5) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(6) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3.9. SELFA processes most data on the grounds of legitimate interest and contract. However, if consent is used as the grounds for processing personal data SELFA will:

a) Clearly and explicitly inform the data subject of all anticipated processing activities at the point of collection (or when the first contact is made if the personal data was not received from the individual).

b) Give the data subject the opportunity to consent to processing prior to undertaking the specified activity.

c) Specify a simple means by which the data subject can exercise their right to "opt out" at any time, should they wish to withdraw consent.

d) Personal data will only be processed in accordance with the activities to which the individual has consented.

3.10. Processing of personal data includes: obtaining, holding, recording, adding, deleting, augmenting, disclosing, destroying, printing or otherwise using data. Processing also includes transferring data to 3rd parties.

3.11. The rights in relation to personal data set out under the GDPR are those of the individual to whom the data relates. Those with 'parental responsibility' are entitled to receive relevant information concerning the child. A child of sufficient maturity and understanding has certain legal rights which the Charity must observe. These include the right to give or withhold consent and certain rights to confidentiality. In exceptional circumstances, if a conflict of interest arises between a parent and a child, the rights of, and duties owed to the child will in most cases take precedence over those of the parent.

4. WHO CAN I SPEAK TO ABOUT DATA PROTECTION ISSUES AT SELFA?

If you have any concerns or questions regarding data protection issues, you can initially speak to your line manager. Your line manager may consult the Senior Administrator or Chief Officer for further advice or clarification.

5. TAKING OWNERSHIP

5.1. The GDPR introduces a new concept called data protection by "design and default". It essentially means that we all have a responsibility to proactively build the principles (set out in paragraphs 3.6 and 3.7 above) into our everyday activities. Don't be afraid to question current or old practices or technology if you think they do not follow good data protection practice and raise any issues or concerns.

6. NEW IDEAS?

6.1. You may want to introduce something new or innovative to the organisation. It could be a new piece of technology or you may be looking to introduce a campaign which involves the use, in some way, of personal data. Or you might want to implement a new piece of software.

6.2. It is important that, before implementing anything new involving or impacting upon personal data, you speak with your line manager. Under the new GDPR concept of data protection by design and default (see paragraph 5), we will need to ensure that we have built good data protection practice into any new idea before implementing the idea. Sometimes, this will require a formal data privacy impact assessment where the new idea is potentially high risk to the privacy of parents, children and/or members of staff.

7. DATA BREACHES

7.1. A personal data security breach is any security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It could be as a result of cybercrime. Or it could be that you, or someone you know, have accidentally shared personal data with another organisation or person without permission.

7.2. If you become aware of a personal data security breach you must inform the Chief Officer immediately, providing as much background detail as possible. This is because the GDPR requires SELFA to report personal data breaches to the regulator within 72 hours of first becoming aware of it. Please do not report the breach to the ICO yourself. Your line manager or the Chief Officer will assist you with completing the breach notification form which will be sent to the ICO.

8. SHARING INFORMATION WITH OTHER ORGANISATIONS

8.1. If you are looking at engaging with any new supplier, and you know that the supplier will be obtaining personal data relating to SELFA service users, parents and/or guardians, members of staff or other groups of people, you will need to contact your line manager as soon as possible before engaging with that supplier.

8.2. The GDPR requires SELFA to (a) vet these suppliers to ensure that they offer an appropriate level of security of personal data and (b) make sure that there is a written contract between the supplier and SELFA and that it is GDPR-compliant before being signed. Your line manager will escalate this as appropriate.

8.3. For the purposes of multi-agency working (e.g. with referrers, schools, the Prevention Service) it may be necessary to share personal data. Who data may be shared with and for what purposes is outlined in SELFA's Privacy Notice. All staff should familiarise themselves with the Notice, and if they have any queries consult their line manager. Where sharing data, staff must be satisfied as to the identity of the person making the request and only provide data where necessary.

8.4. SELFA may share personal data where the GDPR specifies an exemption from non-disclosure provisions, for example where required to share data by order of a court or in

connection with legal proceedings. Further information on exemptions is available on the ICO website www.ico.org.uk.

9. DEALING WITH SUBJECT ACCESS REQUESTS

9.1. A subject access request ("SAR") is a request from an individual to obtain information SELFA holds about him or her. This is a statutory right, however it is not without its complications and doesn't just mean disclosing every piece of information, because there might be legal reasons to withhold certain information. The individual issuing an SAR could be a child, parent and/or guardian of the child, member of staff or member of the public. Not everyone who requests personal data will be entitled to receive it, therefore it is important we verify an individual's right to receive personal data, particularly where the personal data is not about themselves.

9.2. In the case of young children, this right of access will usually be exercised by those with parental responsibility for them. However, even if a child is too young to understand the implications of subject access rights, it is still the right of the child rather than of anyone else such as a parent or guardian.

When receiving a subject access request for information held about a child, you should consider if the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

The important point is whether the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, you should take into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

9.3. As there are strict time periods for complying with a SAR (1 calendar month from the day after the SAR is received), it is important that you immediately notify your line manager who will then assist with the request accordingly. Please do not respond to the

individual without first consulting with your line manager. See Appendix C for further information on responding to a SAR.

10. RIGHT TO ERASURE REQUESTS

10.1. A right to erasure request is a request from an individual to erase information SELFA holds about him or her. Like SARs, this is a statutory right but not as straightforward as you might think and it doesn't just mean deleting every piece of information about the individual because there might be legal reasons to keep certain information. As with SARs, please make sure that you contact your line manager immediately before responding to the individual making the request. Please do not respond to the individual without first consulting your line manager.

11. PROCEDURES FOR HANDLING DATA AND DATA SECURITY

11.1. Under the data protection law, SELFA has a duty to ensure that appropriate technical and organisational measures and training are taken to prevent:

- unauthorised or unlawful processing of personal data
- unauthorised disclosure of personal data
- accidental loss of personal data

11.2. All staff must therefore ensure that personal data is dealt with properly no matter how it is collected, recorded or used. This applies whether or not the information is held on paper or in a computer or recorded by some other means. Staff should consider any information that can be used to identify an individual as personal data and observe the guidance in Operational Guidance (Appendix A) and Data Safety Dos and Don'ts (Appendix B).

12. CHANGES TO THIS POLICY

12.1. We reserve the right to change this policy at any time. Where the changes are significant, we will make sure that we tell you about them.

Change Record

Date of change:	Changed by:	Comments
03/07/2018	Rosie Hall	Police created
17/01/2022	Rosie Hall	Reviewed – some changes to wording to reflect legislation and change of premises. Ratified by Trustees 28.02.2022
19/01/2023	Rosie Hall	Policy reviewed. No changes.

13. Appendix A – Operational Guidance

Email:

All staff should consider whether an email (both incoming and outgoing) will need to be kept as an official record. If the email needs to be retained it should be saved into the appropriate folder or, printed and stored securely. The original email should then be deleted from the personal mailbox and any "deleted items" box, either immediately or when it has ceased to be of use.

Remember, emails that contain personal information which is no longer required for operational use, should be deleted from the personal mailbox and any "deleted items" box.

Phone Calls:

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access.

- Personal information should not be given out over the telephone unless you have no doubts as the caller's identity and the information requested is innocuous. If you have any doubts, ask the caller to put their enquiry in writing.

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be password protected.

Ensure your laptop is locked (password protected) when left unattended, even for short periods of time.

When travelling in a car, make sure the laptop is out of sight, preferably in the boot. If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set. Never leave laptops or portable devices in your vehicle overnight.

Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Personal data received on disk or memory stick should be saved to the relevant

file on the server or laptop. The disk or memory stick should then be securely returned (if applicable) or processed for safe storage or disposal.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords:

Do not use passwords that are easy to guess. Make sure all of your passwords contain both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 8 characters or more in length.

Protect Your Password:

Common sense rules for passwords are:

- do not give out your password
- do not write your password somewhere on your laptop
- do not keep it written on something stored in the laptop case

Tips for a secure password from the National Cyber Security Council are:

- Avoid common passwords such as: password, Password123, P4ssw0rd etc.
- It is recommended to use 3 random words for your password (and a number if required to meet complexity requirements). To help with this, remember that a password can be a 'passphrase' that is easier to remember e.g. Ibuiltasnowmantoday47.
- For really important accounts it is recommended to use 2 factor authentication (a password and another thing that only you have access to, such as a code to be sent to your phone).
- Passwords should not be reused. You should use a different secure password for each site requiring a password.
- Use a password manager where possible. Alternatively, storing passwords in your browser is okay if the device that you are using is not shared with other people.

Data Storage

Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.

Paper records must always be stored securely – for example in the restricted access office premises. If taken out of the office premises records should not be left unattended or where they can be accessed by unauthorised people. When unattended records should be kept locked, for example in a file box or car boot.

Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is our responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

14. Appendix B: Data Safety Dos and Don'ts

Remember:

Data we record about individuals (staff, children, parents etc.) is covered by data protection laws and belongs to that individual. As such, notes we make on databases, in emails and paper records may be seen by the person concerned.

We have access to data as part of our role within the Charity. This data should not be disclosed or used for any purpose that is not official business of the Charity.

Here is a list of 'top tips' when handling Charity data.....

DO ✓

- Record facts and professional opinions only on SELFA records, emails and other similar documents
- Use a strong password on IT systems at work, e.g. a combination of 8 or more alphanumeric characters and symbols
- Change passwords if you believe there is a chance that they have been compromised
- Password protect email attachments containing personal or commercially sensitive data
- Encrypt any removable data devices including USB sticks laptops and similar
- Remember the Charity may incur substantial fines for loss or misuse of data
- Read and familiarise yourself with the Social Media, Internet and Email Policy
- Keep data secure when using it off site
- Think security when posting sensitive documents
- When disposing of documents containing personal data, ensure these are shredded

DON'T X

- Use personal social media with service users
- Contact service users or store pupil/parent contact data on personal devices, e.g. numbers on your mobile
- Don't share passwords
- Don't leave personal data unattended when off site
- Don't create databases of personal data in addition to the official sources

Taking data off site:

- only take offsite information you are authorised to and only when it is necessary
- ensure that it is protected offsite by
    - not leaving it unattended,
    - locking it away when not in use,
    - not discussing or sharing it with non-SELFA staff

- be aware of your location and take appropriate action to reduce the risk of theft
- make sure you sign out completely from any online services you have used e.g. email
- try to avoid other people seeing the information you are working with
- treat records as if they were your bank details and PIN

15. Appendix C – Subject Access Requests

Subject Access Requests can be made verbally or in writing, and can be made to any member of the organisation (including by social media).

If the applicant's request for access is granted, the GDPR requires such access to be given within 1 month of the written request being received. The time limit is from the day after the request is received until the corresponding date in the next month.

In order to meet the 1 month requirement actions given below should be taken:

1. Record receipt of the SAR
2. Send a Subject Access Request Form (Appendix D) to the applicant within two working days of when the request is received by the Charity
3. Forward the completed SAR Form to the Chief Officer
4. Send a written response to the applicant acknowledging receipt of the application form within 5 days of receipt
5. Maintain a SAR process sheet (Appendix E) to identify and monitor deadlines and record contact with and information sent to the applicant. It will also record decisions taken with regard to the application.
6. Collate the data requested and forward the SAR process sheet outlining the information collected and actions taken to the Chief Officer for overview. This must be done within 15 days of the request being received.
7. The Chief Officer must authorise the applicant's request for access before any information is disclosed. The Chief Officer has 10 days from this point to decide the information to be sent (or withheld) to the applicant. The Charity may also wish to get advice from a solicitor in relation to a disclosure.
8. The Charity should agree a secure method of releasing the records to the applicant
9. The applicant should receive the data once the 25 days are complete or sooner if possible. Appendix F has an appropriate cover letter for sending out the data.

Notes

- Where the conditions set out above are fulfilled, in responding to the request, the Charity must give a description of the personal data that is being processed, the purposes for which the personal data is being processed, and the persons to whom the personal data are or may be disclosed.
- The Charity must also provide, in an intelligible form, a copy of the information held and, where possible, details of the source of the information.
- Data subjects are not entitled to information where exemptions to the right of access apply (see 8.4 above). Moreover, in these circumstances, the Charity must only give a notification

to the data subject that no information has been identified which is required to be supplied under the GDPR.

16. Appendix D – Subject Access Request Form

Request for information under the General Data Protection Regulation 2018.

This form should be completed only if you are requesting personal information relating to yourself or on behalf of a third party.

Please complete in block capitals or type.

1. Personal details of the person requesting the information.

Surname:	
Firstname:	
Address:	
Postcode:	
Telephone number:	
Email:	

2. Are you the Data Subject (i.e. the person whose information you are requesting)?

   Please tick the appropriate box

   Yes ☐ (Please go straight to question 5) No ☐

3. Personal details of the Data Subject.

Surname:	
Firstname:	
Address:	
Postcode:	
Telephone number:	
Email:	

4. Please describe your relationship with the Data Subject that leads you to make this request on their behalf.

5. Information requested

   If you would like to see only specific document(s), please describe these below.

   _____

   _____

   _____

   _____

6. If you would like a full copy of the personal records held by the Charity, please tick here ☐

7. Declaration

16.1. I certify that the information given in this application form to SELFA is true. I understand that it will be necessary for SELFA to confirm my/the Data Subject's identity and it may be necessary to supply more detailed information if required.

The details you provide on this form will only be used in connection with your application for the supply of documents and for statistical purposes.

The completed form should be returned to:

SELFA
Ings School
Broughton Road
Skipton
BD23 1TE

admin@selfa.org.uk

SELFA will acknowledge your request within 5 days of receipt and endeavour to complete your request as soon as is practical within the required 1 month period.

Office use only

Initial contact date	
SAR Form received date	
Date to be completed by	
Comments	

17. Appendix E – SAR Process Sheet

Date acknowledged			
Date forwarded to Chief Officer			
Target date for release		Date released	
Verification of subject			

	Description of document	Editing done & reasons given (e.g. third parties anonymised	Signature
Correspondence			
Emails			
Minutes of meetings			
Notes of visits			
Accident forms			
Staff personal file			
Sickness records			
Incident forms			
Referral forms			
Database files			
Other (specify)			

Notes

18. APPENDIX F: SAR Release Letter

[Date]

[Name]

[Address]

Dear [Name of data subject]

Subject Access Request

Thank you for your correspondence of [date] making a data subject access request for [subject].

We are pleased to enclose the information you requested.

We have endeavoured to provide all the information that we hold on the data subject. However, if you have any reason to believe that there is any missing data then please do not hesitate to seek further clarity from us on this matter.

Yours sincerely

Emma Pears
Chief Officer

APPENDIX G: Data Protection Audit Return

Year:

Ref	Description	Current Situation	Status	Action(s)	Owner	Deadline
1.0.	Staff/Service User Records					
1.1.	Service user data is kept in accordance with the data retention policy					
1.2.	Staff data is kept in accordance with the data retention policy					
1.3.	Expired records are disposed of safely and securely by named individuals					
1.4.	All forms used to collect data are identified					
1.5.	All forms used to collect data include the standard SELFA Data Protection disclaimer					
1.6.	Parents are contacted annually to request updates to personal data					
1.7.	All electronic databases in use, including the users, who can access them are identified					
1.8.	Access to all electronic databases is secured by passwords.					
1.9.	All paper record systems in use, for staff or service users, are identified					

1.10.	All paper record systems are secured in accordance with policy guidelines					
1.11.	Staff with access to staff records is documented, controlled and regularly reviewed.					
1.12.	The Accident Forms are used for service users and records are kept for DOB + 25 years (or 40 years if asbestos related).					
1.13.	Accident Forms are used for staff and records are kept for 3 years from the date the incident is logged					
1.14.	All service users, whose parents have opted not to have their photograph used, are clearly identified with the information easily accessible to staff					
2.0.	Procedures					
2.0.	All Service Level Agreements with third party organisations are reviewed to consider data handling compliance					
2.1.	The Charity has a policy in place regarding the use of photography/video by family members at events. The method and frequency of communicating this to parents is documented and completed.					
2.2.	Contact details of parents are not distributed to other parents unless with written consent.					
2.3.	A Subject Access Request (SAR) file is in place to store requests					

3.0.	Staff Training					
3.0.	Staff are made aware of SELFA's Data Protection policy and its implications for them in their work					
3.1.	Staff are made aware that they must inform SELFA of any changes to their personal details e.g. change of address, contact numbers					
3.2.	Have all staff had the minimum training session and been given the DO & DON'T LIST? If not, when is this planned?					

Status key:

Status	Description
	Policy standard not met
	Policy standard partially met. Action Plan in place to achieve full compliance
	Policy standard achieved

Audit completed by:

Signed:

Position:

Date:

19. Appendix H: Parents who wish to use photography and/or video an event

Please note whereas this issue is not subject to the GDPR the Charity needs to have guidelines in place to cover such events.

Generally photographs and videos for Charity and family use are a source of innocent pleasure and pride, which can make children, young people and their families feel good about themselves. By following some simple guidelines we can proceed safely and with regard to the law.

Remember that parents/carers and others, attend Charity events at the invitation of the Chief Officer.

The Chief Officer has the responsibility to decide if photography and videoing of events is permitted.

The Chief Officer has the responsibility to decide the conditions that will apply so that children are kept safe and that the event is not disrupted and children and staff not distracted.

Parents and carers can use photographs and videos taken at a Charity event for their own personal use only. Such photos and videos must not be sold and must not be put on the public facing social media networks.

Recording or/photographing other than for your own private use would require the consent of all the other parents whose children may be included in the images.

Parents and carers must follow guidance from staff as to when photography and videoing is permitted and where to stand in order to minimise disruption to the activity.

Parents and carers must not photograph or video children changing for performances or events.

If you are accompanied or represented by people that staff do not recognise they may need to check who they are, if they are using a camera or video recorder.

Remember that for images taken on mobiles phones the same rules apply as for other photography, you should recognise that any pictures taken are for personal use only.

In exceptional circumstances e.g. child protection orders, the parent and Chief Officer may agree an alternative and practical approach to this policy for specific pupils.